Advanced Ransomware Negotiation Framework

SOCRadar®
Your Eyes Beyond

socradar.io

The Complete Guide: Prevention, Recovery, and Last-Resort Negotiation

Version 2.0 - CISO-Reviewed Edition

Ransomware negotiation is never the preferred outcome. The best strategy is always prevention: resilient backup architecture, strong access controls, network segmentation, continuous monitoring, and a well-trained workforce. However, in certain high-impact scenarios, particularly when backups fail, sensitive data is exfiltrated, or mission-critical operations are at risk, organizations may find themselves with no viable alternative. In those moments, negotiation must be approached strategically, legally, and with disciplined governance, not emotionally or reactively.

This framework reflects more than a decade of frontline cybersecurity and incident response experience. It provides a structured, board-ready decision model that prioritizes prevention and recovery first, and treats negotiation strictly as a last resort. From legal compliance and OFAC screening to technical validation, financial modeling, and executive-level decision support, the goal is to replace chaos with clarity when stakes are at their highest.

Ultimately, this framework exists to strengthen the industry's collective defense posture. By sharing hard-earned lessons, operational tactics, and governance strategies, we aim to reduce successful attacks, minimize damage when incidents occur, and ensure that when organizations are forced into difficult decisions, they act responsibly, strategically, and in the best interest of their stakeholders, while continuing the broader fight against cybercriminal ecosystems.

Ensar Seker (PhD)

Chief Information Security Officer (CISO), SOCRadar

CRITICAL LEGAL & ETHICAL WARNINGS

READ THIS BEFORE PROCEEDING:

Legal Warnings

- Paying sanctioned entities is a FEDERAL CRIME with personal criminal liability for executives.
- OFAC violations carry fines up to $20M+ per violation and potential imprisonment.
- Insurance fraud, such as misrepresenting positions, may void coverage.
- Fiduciary duty violations if the payment decision is not properly justified to the board.
- Securities violations for public companies failing to disclose material incidents.

Ethical Considerations

- You are funding criminal enterprises that attack hospitals, schools, and critical infrastructure.
- Your payment incentivizes future attacks on other organizations.
- Criminal groups have documented ties to terrorist organizations and nation-states.
- Payment does not guarantee success - decryptors fail, reinfections occur, and data still leaks.

Framework Limitations

- This framework should be reviewed by legal counsel before use.
- Success is not guaranteed even with perfect execution.
- Alternative recovery methods should ALWAYS be exhausted first.
- Prevention is 100x more effective than response.
- Every situation is unique - adapt this framework to your context.

If you are currently in an active ransomware incident, skip to Phase 1. If you are reading this for preparation, start with Phase 0.

PHASE 0: PREVENTION & PREPARATION

Philosophy: The best ransomware negotiation is one you never have to conduct.
Organizations with strong prevention and backup strategies rarely pay ransoms. Investment here pays 100:1 returns compared to incident response costs.

0.1 Critical Prevention Controls

Tier 1: Backup Architecture (Non-Negotiable)

Implementation Requirements:

Daily Backups:

- Full system backups of all critical systems
- Application-consistent backups (not just file-level)
- Database transaction log backups (every 15-30 minutes)
- Configuration backups of network devices
- Automated backup verification and integrity checks

Immutable/Air-Gapped Storage:

- Physically disconnected backup media (tape libraries, removable drives)
- Object storage with immutability (AWS S3 Object Lock, Azure Immutable Blobs)
- Write-once-read-many (WORM) storage appliances
- Separate authentication domain (not accessible with domain admin credentials)

Backup Security:

- Backups stored on separate network segments
- Separate administrative credentials (not shared with production AD)
- MFA required for backup system access
- Backup integrity monitoring with alerting
- Regular restore testing (monthly minimum)

Recovery Time Testing:

- Document actual recovery times (not vendor promises)
- Full disaster recovery test quarterly
- Tabletop exercises monthly
- Know your Recovery Time Objective (RTO) for critical systems
- Know your Recovery Point Objective (RPO) - maximum acceptable data loss

Critical Success Metric: "Can we restore our entire environment from backups in 72 hours or less without paying ransom?"

If the answer is NO, you have a critical vulnerability.

Tier 2: Access Control & Authentication

Multi-Factor Authentication (MFA):

- Required on ALL remote access (VPN, RDP, SSH)
- Required on ALL administrative accounts
- Required on email (Office 365, Google Workspace)
- Required on cloud management consoles (AWS, Azure, GCP)
- Hardware tokens preferred over SMS (SIM swapping attacks)
- Conditional access policies based on location/device

Privileged Access Management (PAM):

- Dedicated PAM solution (CyberArk, BeyondTrust, Delinea)
- No standing administrative privileges
- Just-in-time elevation with approval workflows
- Session recording for all privileged access
- Automatic password rotation every 24-48 hours
- Break-glass accounts in secure physical location

Network Access Control:

- VPN required for ALL remote access (no direct RDP/SSH to internet)
- Certificate-based VPN authentication
- Device compliance checks before network access
- Network admission control (NAC) for internal access

Critical Items to Disable:

- RDP exposed directly to internet (use VPN or jump boxes)
- Default administrative accounts (rename or disable)
- Legacy authentication protocols (NTLMv1, SMBv1)
- Unnecessary remote access services

Tier 3: Endpoint & Network Protection

Endpoint Detection & Response (EDR):

- Deploy EDR on 100% of endpoints and servers
- Leading solutions: CrowdStrike, Microsoft Defender for Endpoint, SentinelOne
- 24/7 monitoring with automatic response enabled
- Block unknown executables on servers
- Ransomware-specific behavioral detection
- Automatic isolation of infected endpoints

Network Segmentation:

- Separate networks for: Production, Development, Corporate, Guest, OT/ICS
- Firewall rules between segments (deny-by-default)
- Micro-segmentation for critical assets
- Separate authentication domains when possible
- Critical servers on isolated VLAN with strict access controls

Application Whitelisting:

- Deploy on all servers (Microsoft AppLocker, Carbon Black)
- Only approved applications can execute
- Blocks ransomware executables automatically
- Significantly reduces attack surface

Email Security:

- Advanced threat protection (ATP) enabled
- Block executable attachments (.exe, .scr, .bat, .ps1, .js, .vbs)
- Link scanning and sandboxing
- DMARC, SPF, DKIM configured correctly
- Security awareness training quarterly

Vulnerability Management:

- Patch critical vulnerabilities within 72 hours
- Automated patch deployment where possible
- Focus on internet-facing systems first (VPN appliances, web servers)
- Virtual patching for legacy systems that can't be patched
- Monthly vulnerability scanning

Tier 4: Detection & Response Capability

Security Information & Event Management (SIEM):

- Centralized log collection from all systems
- Retention: 90 days hot storage, 1 year archive
- Correlation rules for ransomware indicators
- Failed login alerts (10+ failures in 30 minutes)
- Off-hours administrative activity alerts
- Lateral movement detection

Key Logs to Collect:

- Windows Security Event Logs (especially Event IDs 4624, 4625, 4672, 4688)
- VPN authentication logs
- Firewall connection logs
- DNS query logs
- Cloud service logs (AWS CloudTrail, Azure Activity Log)
- EDR telemetry

Incident Response Preparation:

- Documented incident response plan (tested quarterly)
- Dedicated incident response team with defined roles
- 24/7 on-call rotation
- Communication plan templates (internal and external)
- Pre-established relationships with IR firms
- Cyber insurance policy with understood coverage
- Legal counsel with cyber expertise on retainer

Ransomware-Specific Playbook:

- Immediate containment procedures
- Forensic evidence preservation steps
- Communication trees (phone-based, email may be down)
- Decision authority matrix (who approves what)
- Pre-approved budget for emergency response
- List of pre-vetted vendors (IR firms, PR firms, legal counsel)

0.2 Pre-Incident Preparation Checklist

Complete These Actions NOW (Before Incident):

Legal & Insurance

- ☐ Cyber insurance policy purchased with understood coverage limits
- ☐ Policy covers: Ransom payment, forensics, business interruption, legal costs, notification
- ☐ Exclusions understood (war, prior acts, failure to maintain security)
- ☐ Insurance broker contact information documented
- ☐ Cybersecurity legal counsel identified and contacted
- ☐ OFAC compliance attorney contact information documented
- ☐ Retainer agreement with incident response firm

Financial

- ☐ Cryptocurrency exchange account opened and verified (Coinbase/Kraken/Gemini)
- ☐ Bank account linked to crypto exchange
- ☐ Purchase limits increased to required level
- ☐ Hardware cryptocurrency wallet purchased (Ledger/Trezor)
- ☐ CFO/Treasury has process to authorize emergency payments
- ☐ Board has pre-approved emergency incident response budget

Technical

- ☐ Complete backup inventory with RTO/RPO documented
- ☐ Backup restoration tested in last 90 days
- ☐ Backup systems isolated from production network
- ☐ Forensic evidence collection procedures documented
- ☐ Network segmentation diagram current
- ☐ Critical systems inventory maintained
- ☐ Offline copy of network diagrams and passwords (in physical safe)

Communication

- [ ] Crisis communication plan documented
- [ ] Phone tree established (alternative to email)
- [ ] PR firm contact information documented
- [ ] Customer notification templates prepared
- [ ] Regulatory notification templates prepared
- [ ] Media response guidelines documented
- [ ] Social media monitoring plan

Governance

- [ ] Board briefed on ransomware risks and response options
- [ ] Payment vs. non-payment decision criteria agreed
- [ ] Ethical considerations discussed and documented
- [ ] Decision authority clearly defined
- [ ] Fiduciary responsibilities understood

How Many Boxes Did You Check?

- **20+:** You're well-prepared
- **10-19:** Significant gaps remain
- **<10:** You're at high risk - prioritize preparation immediately

PHASE 1: IMMEDIATE RESPONSE (Hours 0-24)

Detection, Containment, and Initial Assessment

DO NOT contact threat actors yet. You need situational awareness first.

1.1 Initial Detection & Confirmation

Ransomware Indicators

- Mass file encryption events (file extensions changed, files inaccessible)
- Ransom notes appearing on systems (text files, desktop wallpaper changes)
- Unusual network traffic patterns (encrypted file shares, lateral movement)
- System performance degradation (encryption is CPU-intensive)
- Security tool alerts (EDR/antivirus detections)
- User reports of inaccessible files
- Backup deletion or modification events

Immediate Triage Questions

1. How many systems are affected? (Don't rely on initial reports - assume more)
2. Is encryption still actively spreading? (Watch for new infections)
3. Are backups intact? (Check immediately - they're usually targeted)
4. Is data being exfiltrated? (Network monitoring, unusual outbound traffic)
5. What are the business impacts? (Revenue loss, operational disruption)

1.2 Immediate Containment Actions

Execute within 1-2 hours

Network Isolation (DO THIS FIRST)

Immediate Actions:

1. Disconnect affected network segments at switch/router level
    - Physical disconnection if possible
    - Disable VLANs/network ports
    - Block at firewall
2. Disable ALL domain admin accounts
    - Assume credentials are compromised
    - Create new emergency admin accounts
    - Use local accounts on critical systems temporarily
3. Shut down or isolate domain controllers
    - If credential compromise suspected
    - Run from backed-up domain controller if available
    - Prevents spread via Active Directory replication
4. Disable remote access
    - VPN servers offline
    - RDP gateways disabled
    - Any other remote access methods blocked
5. Isolate backup systems
    - Disconnect backup servers from network
    - Prevent backup destruction
    - Verify backup integrity immediately

What **NOT** to shut down:

- Security monitoring tools (you need visibility)
- Forensic evidence sources (preserve logs)
- Critical safety systems (industrial controls, medical devices)
- Systems that could cause physical harm if suddenly stopped

Evidence Preservation

Immediate Forensic Actions:

1. Memory Dumps (before rebooting anything)
    - Capture RAM from infected systems
    - Contains encryption keys, attacker tools, process information
    - Tools: FTK Imager, WinPMEM, Magnet RAM Capture
2. Log Preservation
    - Export all security event logs immediately
    - Firewall logs (30 days if possible)
    - VPN authentication logs
    - DNS query logs
    - Cloud service logs
    - EDR/antivirus logs

3. Disk Imaging (if time permits)
    - Image critical systems before making changes
    - Forensic bit-for-bit copies
    - Maintain chain of custody
    - Store on separate, secured media
4. Network Capture
    - Begin packet capture on key network segments
    - May capture command-and-control traffic
    - May reveal data exfiltration

Why This Matters:

- Evidence degrades rapidly (logs roll over, memory cleared, systems rebooted)
- Law enforcement investigation requires evidence.
- Insurance claims require documentation.
- Forensic analysis needs untainted evidence.

Communication Lockdown

Internal Communications:

- DO NOT use company email (may be compromised or down)
- Establish phone-based communication trees
- Use personal phones/external messaging (Signal, WhatsApp) for sensitive discussions
- Create dedicated Slack/Teams workspace on separate tenant if needed

External Communications:

- Lock down social media immediately
    - Brief employees not to post about incident
    - Monitor social media for leaks
    - Prepare holding statements
- Control information flow
    - Need-to-know basis only
    - Avoid creating panic
    - Consistent messaging

1.3 Rapid Scope Assessment

Hours 2-12

Encryption Scope

Number of systems encrypted
Types of systems (servers, workstations, cloud, mobile)
Critical systems affected (production databases, ERP, email)
Encryption progress (still spreading or contained?)
File types encrypted (documents, databases, backups, system files)

Data Exfiltration Assessment

Critical Question: Did they steal data before encrypting?

Indicators of Exfiltration:

- Large outbound data transfers (TB-scale to external IPs)
- Unusual cloud storage uploads (Mega, RapidShare, etc.)
- FTP/SFTP connections to unknown destinations
- Tor network usage
- Unusual compression/archiving activity before encryption
- Explicit claims in ransom note: "We have stolen X GB of your data"

Check These Logs:

- Firewall egress logs (last 30-60 days)
- DLP alerts
- Cloud access security broker (CASB) logs
- Proxy logs
- Network flow data (NetFlow, IPFIX)

Why This Matters:

- Encryption alone = recovery from backups viable
- Data theft (double extortion) = payment may be necessary to prevent leak
- Changes entire decision calculus

Backup Status Assessment

CRITICAL: Verify backup integrity immediately.

Assessment Questions:

1. Are backups encrypted?
    - Check backup repository directly
    - Attempt test restore of sample files
    - Verify backup metadata hasn't been corrupted
2. How recent are unencrypted backups?
    - Last successful backup timestamp
    - Recovery Point Objective (RPO) - how much data loss is acceptable?
3. Are backups complete?
    - All critical systems included?
    - Application-consistent (databases, email)?
    - Configuration data included?
4. Can we actually restore?
    - Test restore small subset
    - Verify restored data integrity
    - Estimate full restoration time

Backup Scenarios:

Scenario	Implications	Recommended Path
Backups intact and recent	Can restore without payment	Recovery Path - Don't negotiate
Backups partially encrypted	Can restore some systems	Hybrid approach - negotiate only for encrypted backup data
Backups completely encrypted	Cannot restore	Negotiation Path - but verify this thoroughly first
Backups missing/corrupt	Major problem	Negotiation Path - but also investigate why backups failed

Common Ransomware Backup Attacks:

- Vssadmin delete shadows (deletes Windows Volume Shadow Copies)
- Backup service credential theft
- Backup repository encryption
- Backup catalog corruption
- Backup job deletion

Threat Actor Identification

Analyze Ransom Note:

- Ransomware family (file extension, note signature, wallpaper)
- Communication channels provided (.onion URL, Tox ID, email)
- Ransom amount and payment deadline
- Specific language/phrasing (may indicate group)
- Leak site mentioned (double extortion indicator)

Cross-Reference with Threat Intelligence:

- ID Ransomware (https://id-ransomware.malwarehunterteam.com)
- Upload encrypted file sample + ransom note
- Identifies specific ransomware family
- May indicate known decryptors available

Check for Free Decryptors:

- No More Ransom Project (https://www.nomoreransom.org)
- Free decryption tools for some ransomware families
- Must identify exact variant correctly
- Test on isolated system first

OFAC Sanctioned Groups (DO NOT PAY WITHOUT LEGAL REVIEW):

- Evil Corp (Dridex gang)
- Conti (and successors/rebrands)
- DarkSide/BlackMatter
- North Korean groups (Lazarus, etc.)
- Sanctions list evolves - check current OFAC SDN list

Research Group Reputation:

- Do they actually provide working decryptors?
- What percentage of victims report successful decryption?
- Are they known to return for a second payment?
- Check forums: BleepingComputer, Reddit r/ransomware

1.4 Critical Notifications (First 4 Hours)

Immediate Notifications Required:

Internal Stakeholders

1. CEO/President (within 1 hour)
    - Brief situation overview
    - Initial scope assessment
    - Expected business impacts
    - No decisions required yet - just awareness
2. CFO (within 1 hour)
    - Financial impact estimates
    - Potential ransom amounts
    - Insurance policy activation
    - Budget authorization for response costs
3. General Counsel (within 1 hour)
    - Legal/regulatory implications
    - OFAC compliance concerns
    - Notification obligations
    - Attorney-client privilege protection
4. Board of Directors (within 2-4 hours)
    - High-level briefing
    - Material incident determination
    - Fiduciary responsibilities
    - Major decisions upcoming
5. Incident Response Team (immediately)
    - Activate response team
    - Assign roles and responsibilities
    - Establish communication channels
    - Begin executing containment

External Stakeholders

Insurance Carrier **(WITHIN 1 HOUR - CRITICAL)**:

- Cyber insurance policy activation
- Failure to notify promptly = claim denial risk
- Provides access to:
    - Pre-approved incident response firms
    - Legal counsel
    - Negotiation specialists
    - Public relations firms
- Request panel counsel list immediately
- Document notification time precisely

Insurance Claim Immediate Actions:

- Call broker and carrier simultaneously
- Request claim number
- Ask for approved vendor list
- Document all communications
- Follow policy notification procedures exactly

Law Enforcement (Within 24 Hours - Recommended):

FBI Notification Benefits:

- Access to threat intelligence on attacker group
- Known decryption keys (if available)
- Bitcoin wallet tracking/potential recovery
- OFAC compliance documentation
- No cost for assistance

How to Report:

- FBI Internet Crime Complaint Center (IC3): https://ic3.gov
- FBI local field office cyber squad
- Secret Service if financial sector
- CISA (if critical infrastructure)

What to Provide:

- Ransom note
- IOCs (IP addresses, file hashes, Bitcoin wallets)
- Timeline of events
- Scope of compromise

What NOT to worry about:

- LE understands business necessity of payment
- LE focuses on catching criminals, not victims
- Your report likely won't result in investigation that impacts you
- Benefits far outweigh any perceived risks

Legal Counsel Specializing in Cyber (Immediately):

- Establish attorney-client privilege
- OFAC compliance review
- Regulatory notification requirements
- Communication strategy
- Payment authorization legal review

DO NOT Notify Yet:

- Customers (until you understand scope)
- Media (unless legally required)
- Regulators (unless immediate notification required)
- Business partners (until containment confirmed)

Premature notification risks:

- Incomplete information leading to confusion
- Unnecessary panic
- Competitive disadvantage
- Stock price impact (public companies)

1.5 Initial Business Impact Assessment

Calculate Expected Costs:

Direct Costs

- Lost Revenue: $____/day × _____ days = $_____
- Incident Response: IR firm, forensics, legal ($500K-$2M typical)
- Ransom Payment: Demanded amount × negotiation factor (30-50% typical)
- System Restoration: IT staff overtime, vendor costs, replacement hardware
- Regulatory Fines: GDPR, state laws, industry-specific (highly variable)
- Customer Notification: Letters, credit monitoring ($3-5 per customer)

Indirect Costs

- Customer Churn: % lost customers × customer lifetime value
- Reputation Damage: Hard to quantify but real
- Insurance Premium Increases: 20-50% increases common post-incident
- Lost Productivity: Employee downtime, workarounds
- Opportunity Costs: Missed deals, delayed projects

Regulatory/Compliance Impacts

- GDPR (EU): 72-hour notification if personal data affected (up to €20M or 4% revenue fine)
- HIPAA (Healthcare): 60 days to notify individuals (up to $1.5M annual fine per violation type)
- State Breach Laws: Varies by state (California: 500+ residents = Attorney General notification)
- SEC (Public Companies): Material incidents within 4 business days
- Industry-Specific: Financial (FINRA), Energy (TSA), etc.

Total Estimated Incident Cost: $_____

This number drives the payment vs. recovery decision.

PHASE 2: STRATEGIC DECISION POINT (Hours 12-48)

Pay vs. Recover - The Most Critical Choice

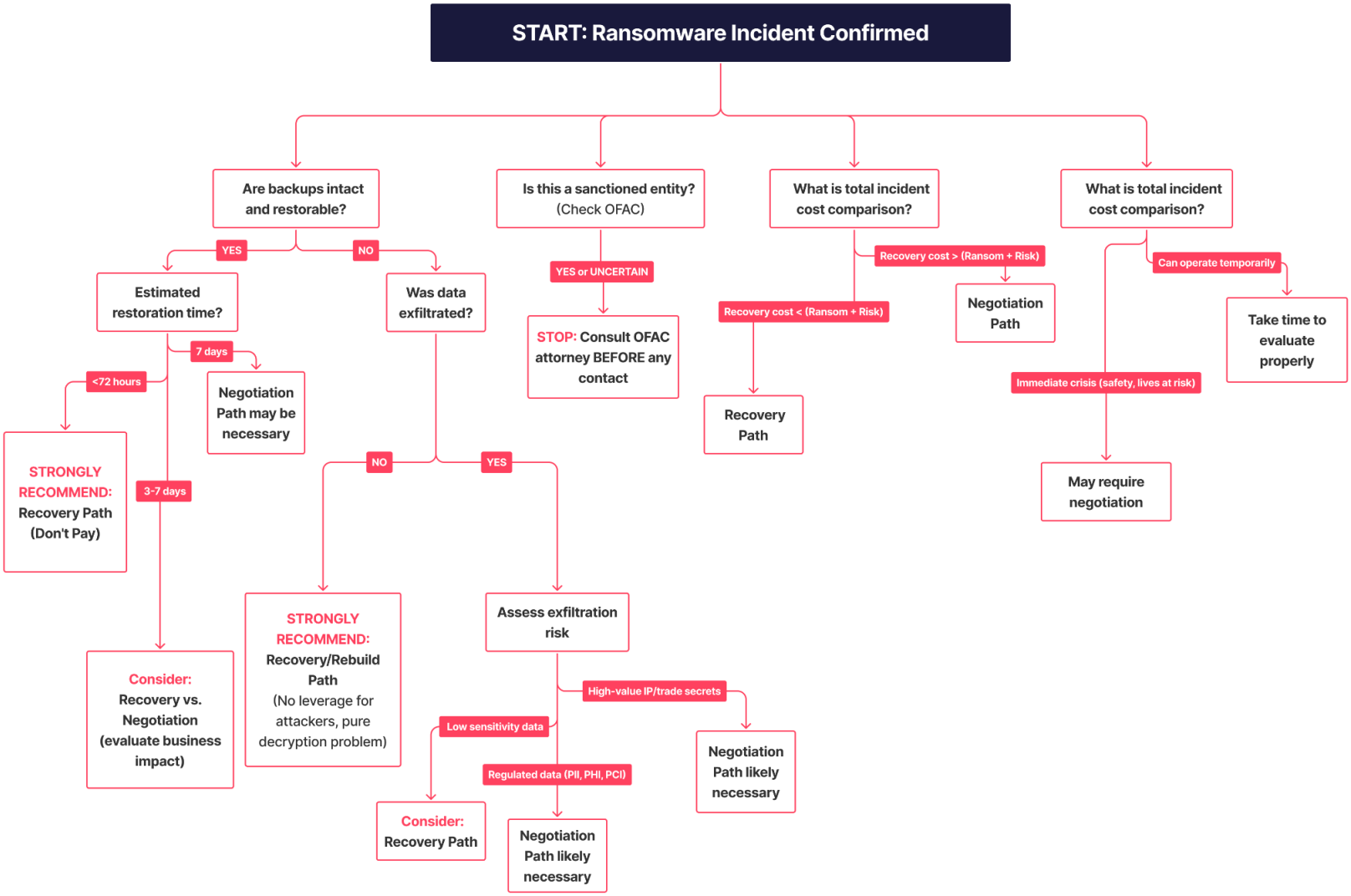
DO NOT rush this decision. Taking 24-48 hours to make an informed choice is better than hasty action.

2.1 Decision Framework

The Core Question

"Can we recover operations and protect our stakeholders without paying the ransom?"

Decision Tree



2.2 Recovery Path (Non-Payment) Assessment

When Recovery Without Payment is Viable:

Scenario A: Backups Intact, No Data Exfiltration

Strongest Position - **RECOMMENDED PATH**

Advantages:

- ✅ No funding of criminal enterprise
- ✅ No OFAC compliance risks
- ✅ No payment sets precedent for future attacks
- ✅ Demonstrates resilience to stakeholders
- ✅ Insurance covers recovery costs
- ✅ Law enforcement can work freely

Requirements:

- Verified backup integrity
- Acceptable Recovery Time Objective (RTO)
- No sensitive data stolen
- Ability to operate during restoration

Actions:

- Begin restoration immediately
- Do NOT contact threat actors
- Focus all resources on recovery
- Enhance security during rebuild
- Full forensic investigation parallel to recovery

Scenario B: Partial Backups, Low-Sensitivity Data Exfiltration

Strong Position - **OFTEN RECOMMENDED**

Considerations:

- Restore what you can from backups
- Rebuild systems without backups
- Accept data loss on less critical systems
- Negotiate ONLY if data leak creates unacceptable risk

Risk Assessment for Data Leak:

- What data was stolen? (Review exfiltration evidence)
- Who is harmed if leaked? (Customers, employees, partners?)
- What are regulatory implications? (GDPR, HIPAA, state laws?)
- What is reputational damage? (Depends on industry, visibility)
- Can we proactively notify affected parties? (Reduces leak leverage)

Scenario C: Wiper Attack Disguised as Ransomware

NO PAYMENT POSSIBLE

Indicators:

- No functional communication channel
- Implausibly high ransom demands
- Suspiciously timed with geopolitical events
- Technical analysis shows no decryption mechanism
- Targets align with nation-state interests

Response:

- Recovery/rebuild is ONLY option
- Report to FBI/CISA immediately
- Treat as destructive attack, not ransomware
- Focus on attribution for potential legal action

2.3 Negotiation Path (Payment) Assessment

When Payment May Be Necessary:

Scenario A: Double Extortion with High-Value Data

Payment Often Necessary

Conditions:

- Significant sensitive data stolen AND verified
- Data leak would cause catastrophic harm:
  - Mass PII/PHI exposure with regulatory fines
  - Trade secrets or competitive information
  - Customer trust irreparably damaged
  - Legal liability exposure (lawsuits)
- Recovery from backups possible BUT doesn't address data leak risk

Note: You're paying for data deletion promise (unverifiable), not decryption

Scenario B: No Viable Backups + Mission-Critical Operations

Payment May Be Necessary

Conditions:

- Backups encrypted/destroyed/never existed
- Restoration would take weeks/months
- Business cannot survive downtime
- Examples:
  - Healthcare (patient care impacted)
  - Manufacturing (supply chain obligations)
  - Financial services (regulatory requirements)
  - Critical infrastructure

Note: This represents a backup failure - learn from it

Scenario C: Safety or Life-Critical Systems

Payment May Be Immediately Necessary

Conditions:

- Healthcare systems affecting patient care
- Industrial control systems with safety implications
- Emergency services systems
- Situations where delay could cause harm

Note: These require immediate decision-making with different criteria

2.4 Financial Analysis

Total Cost Comparison Model

Recovery Path Costs:

None

Personnel Costs:
- IT staff overtime: _____ hours × $_____ = $_____
- Outside consultants: _____ days × $_____ = $_____
- Forensics firm: $_____
- Legal counsel: $_____

Technology Costs:
- Hardware replacement: $_____
- Software licenses: $_____
- Cloud resources: $_____
- Security tools: $_____

Business Impact:
- Revenue loss: $_____/day × _____ days = $_____
- Contract penalties: $_____
- Customer churn (estimated): $_____
- Opportunity costs: $_____

Regulatory/Legal:
- Notification costs: $_____
- Regulatory fines (estimated): $_____
- Legal settlements (estimated): $_____

TOTAL RECOVERY COST: $_____

Negotiation/Payment Path Costs:

None

Ransom Payment:
- Initial demand: $_____
- Expected negotiated amount (30-50% of demand): $_____
- Cryptocurrency transaction fees (3-5%): $_____

Response Costs:
- Incident response firm: $_____
- Negotiation specialist: $_____
- Forensics: $_____
- Legal counsel (including OFAC): $_____

Recovery Costs:
- Decryption + validation: $_____
- System rebuilding (decryption incomplete): $_____
- Security hardening: $_____

Business Impact:
- Revenue loss during decryption: $_____/day × _____ days = $_____
- Reduced but not eliminated

Regulatory/Legal:
- Notification costs (if data stolen): $_____
- Potential fines: $_____
- Reputational damage: $_____

Risk Factors:
- Decryptor may not work (10-15% failure rate): $_____
- Reinfection risk (80% within 12 months): $_____
- Data leaked anyway (30% of payments): $_____

TOTAL PAYMENT PATH COST (Expected): $_____
TOTAL PAYMENT PATH COST (Worst Case): $_____

Decision Matrix:

Criterion	Recovery Path	Payment Path	Weight
Financial cost	$____	$____	30%
Time to operations	___ days	___ days	25%
Data protection	✓ No leak	? Uncertain	20%
Legal risk	Low	Medium-High (OFAC)	15%
Ethical considerations	✓ Clean	× Funds criminals	10%

Weighted Score: Recovery = _____ vs. Payment = _____

2.5 Board Decision Meeting

Prepare Board Decision Package:

Executive Summary (1 page)

- Incident overview
- Current status
- Two path options with pros/cons
- Financial comparison
- Recommended path with justification
- Decision required and timeline

Detailed Briefing Materials

- Technical incident analysis
- Backup status assessment
- Data exfiltration analysis
- Cost-benefit analysis
- Legal/regulatory implications
- OFAC compliance assessment
- Insurance coverage details
- Recommended decision with rationale

Key Questions to Answer for Board

1. "Why didn't our security prevent this?"
    - Honest assessment of security gaps
    - Contributing factors (budget constraints, staffing, legacy systems)
    - What we've learned
    - Prevention plan going forward
2. "If we pay, will this solve the problem?"
    - Payment provides decryptor (maybe)
    - Payment does NOT guarantee:
        - Decryptor will work properly
        - Data will actually be deleted
        - They won't attack us again
        - They won't sell our data anyway
    - Success rate: ~85-90% get working decryptor, ~70% avoid data leak
3. "What are the legal risks of paying?"
    - OFAC sanctions (criminal liability if sanctioned entity)
    - Potential insurance fraud if misrepresent situation
    - Fiduciary duty considerations
    - Securities law (material non-disclosure for public companies)
    - No legal risk for paying non-sanctioned actors (though ethically questionable)
4. "What happens if we don't pay and data leaks?"
    - Regulatory notifications required (GDPR, state laws, HIPAA)
    - Notification costs: $3-5 per affected individual
    - Regulatory fines (highly variable, depends on jurisdiction and negligence)
    - Civil lawsuits (class actions common for PII breaches)
    - Customer trust / reputation damage
    - Insurance may cover some costs
    - May be less costly than paying + experiencing leak anyway (30% of cases)
5. "How long until we're back to normal operations?"

Recovery Path:

- Critical systems: ___ days
- Full operations: ___ days
- Complete remediation: ___ weeks

Payment Path:

- Payment to decryptor receipt: 1-3 days
- Decryption completion: ___ days to ___ weeks
- Validation and stabilization: ___ days
- Complete remediation: ___ weeks

6. "What's your recommendation and why?"

Template Response: "Based on our analysis, I recommend [PATH] because:

1. [Primary rationale - financial, operational, or ethical]
2. [Supporting factor]
3. [Risk mitigation provided by this path]

This decision is not without risks. [Acknowledge key risks of recommended path]

However, compared to the alternative [OTHER PATH], which carries risks of [key risks of alternative], this represents the most responsible path forward for [stakeholders, shareholders, customers].
I need the board's authorization to proceed with [PATH] and budget approval of approximately $_____ for incident response costs."

Board Resolution Template

None

UNANIMOUS WRITTEN CONSENT OF THE BOARD OF DIRECTORS
[COMPANY NAME]

RESOLVED, that the Board of Directors, having been briefed on the ransomware incident affecting company systems beginning on [DATE], and having considered the financial, operational, legal, and ethical implications of response options, hereby authorizes management to:

[IF RECOVERY PATH]
1. Proceed with system restoration from backups without engaging in ransom payment negotiations
2. Expend up to $_____ for incident response, forensics, and recovery costs
3. Engage law enforcement and regulatory authorities as legally required
4. Implement enhanced security measures to prevent recurrence

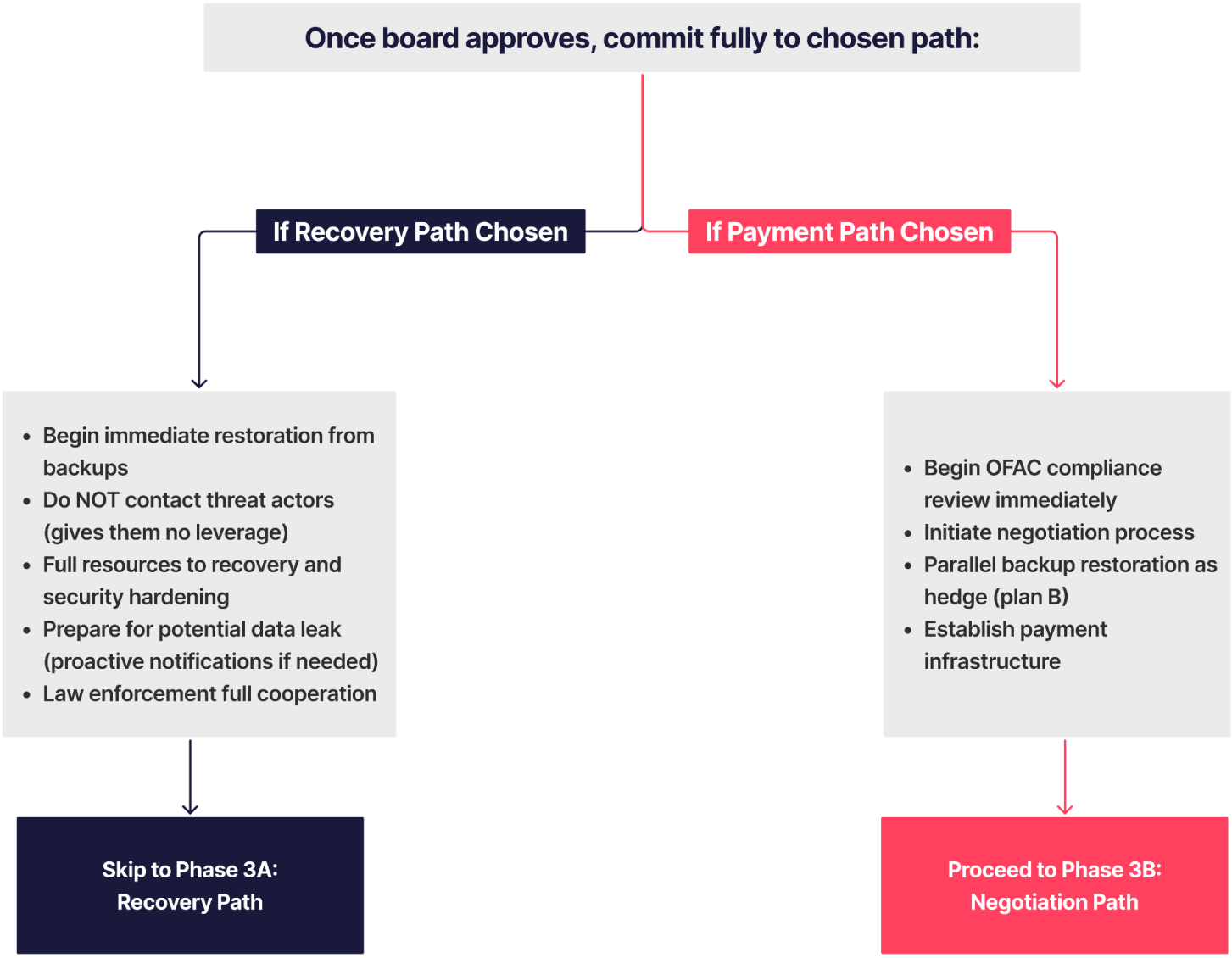
[IF PAYMENT PATH]
1. Proceed with ransom negotiation with the goal of achieving payment of no more than $_____
2. Engage OFAC compliance counsel to ensure payment legality
3. Expend up to $_____ for incident response, negotiation, forensics, and recovery costs
4. Make payment only after:
   a. OFAC compliance clearance obtained
   b. Test decryption successful
   c. Legal counsel approval
5. Implement enhanced security measures to prevent recurrence

FURTHER RESOLVED, that management is directed to provide daily updates to the Board during active incident response and weekly updates thereafter until
full resolution.

Dated: [DATE]

2.6 The Decision: Commit to a Path

Once board approves, commit fully to chosen path:



PHASE 3A: RECOVERY PATH (Non-Payment)

Restoration, Hardening, and Resilience

This phase assumes you have chosen NOT to pay ransom and will recover independently.

3A.1 Backup Restoration Strategy

Restoration Prioritization

Tier 1: Critical Business Systems (Restore First)

- Systems required for revenue generation
- Customer-facing services
- Production databases
- Email/communication systems
- Financial systems
- Estimated restoration time: _____ hours

Tier 2: Important Supporting Systems

- Internal applications
- File servers
- Collaboration tools
- HR systems
- Estimated restoration time: _____ days

Tier 3: Nice-to-Have Systems

- Archive data
- Development/test environments
- Historical records
- Estimated restoration time: _____ weeks

Restoration Execution

Phase 1: Isolated Testing (Hours 0-8)

1. Verify backup integrity
    - Test restore to isolated network
    - Validate data completeness
    - Check application functionality
    - Document any corruption or gaps
2. Build clean infrastructure
    - New domain controllers (if domain compromised)
    - Fresh operating systems
    - Updated security configuration
    - Network segmentation implemented
3. Test restoration process

- Restore one system of each type
- Validate functionality
- Document issues and workarounds
- Estimate completion times

Phase 2: Staged Production Restoration (Days 1-5)

Day 1-2: Core Infrastructure

- Domain controllers (if applicable)
- DNS servers
- DHCP servers
- Network monitoring
- Security tools (SIEM, EDR)

Day 2-3: Critical Business Systems

- Production databases
- Application servers
- Web servers
- Payment processing

Day 3-4: Communication Systems

- Email servers (Exchange, Gmail)
- Collaboration platforms (SharePoint, Teams)
- Phone systems

Day 4-5: User Environment

- File servers
- Workstations (phased approach)
- Printers and peripherals

Phase 3: Validation and Stabilization (Days 5-10)

- Application testing
- User acceptance testing
- Performance monitoring
- Issue resolution
- Documentation updates

Common Restoration Challenges

Challenge: Backup Doesn't Include Everything

- Solution: Rebuild missing components from scratch
- Document what was lost
- Assess business impact
- Prioritize rebuilds

Challenge: Database Corruption in Backups

- Solution: Restore to last known good backup (older)
- Accept data loss
- Attempt database repair tools (high risk)
- Manual data reconstruction if critical

Challenge: Application Configuration Lost

- Solution: Manual reconfiguration required

- Engage vendors for support
- Document configurations going forward
- Consider configuration management tools

Challenge: Restored Systems Reinfected

- Solution: Initial access vector not eliminated
- Return to forensics
- More aggressive containment
- May require complete rebuild rather than restore

3A.2 Alternative: Complete Rebuild Strategy

When Backups Are Insufficient or Unreliable

The "Scorched Earth" Approach

Advantages:

- Guaranteed clean environment
- Opportunity to improve architecture
- Eliminates any persistence mechanisms
- Forces security best practices
- Modern configuration from start

Disadvantages:

- Longer timeline (weeks to months)
- Higher costs (staff time, licenses)
- Significant business disruption
- Potential data loss
- Complex project management

Rebuild Execution Plan

Phase 1: Architecture Design (Week 1)

1. Design improved architecture
    - Network segmentation
    - Zero-trust principles
    - Cloud vs. on-premise decisions
    - Disaster recovery improvements
2. Acquire resources
    - Hardware procurement
    - Software licenses
    - Cloud resources
    - Staff augmentation
3. Build parallel environment
    - Don't dismantle old until new works
    - Isolated network for building
    - Fresh installations

Phase 2: Infrastructure Build (Weeks 2-4)

1. Core infrastructure
    - New Active Directory domain (if compromised)
    - Network infrastructure
    - Storage systems
    - Backup systems
2. Security foundation
    - EDR deployment
    - SIEM implementation
    - MFA infrastructure
    - PAM solution
3. Application layer
    - Database installations
    - Application servers
    - Web servers
    - Integration middleware

Phase 3: Data Migration (Weeks 4-8)

1. Data extraction
    - Extract data from encrypted systems (if possible)
    - Scan extracted data for malware
    - Clean and validate data
    - Import into new systems
2. Data loss assessment
    - Identify unrecoverable data
    - Business impact analysis
    - Alternative data sources
    - Manual reconstruction

Phase 4: Cutover and Validation (Weeks 8-12)

1. User migration
    - Phased approach by department
    - Training on any changes
    - Support resources
2. Validation
    - Functionality testing
    - Performance testing
    - Security validation
    - User acceptance

3A.3 Data Leak Response (If Applicable)

If threat actors stole data and you chose not to pay:

Proactive Notification Strategy

The Logic:

- Threat actors will likely leak data if you don't pay
- Proactive notification reduces their leverage
- Demonstrates responsibility to stakeholders
- Better than reactive scramble after leak
- May reduce regulatory penalties (good faith effort)

Notification Process

Week 1: Legal Review and Preparation

1. Determine notification obligations
    - GDPR: 72 hours to supervisory authority, without undue delay to individuals
    - State laws: Varies by state (typically 30-90 days)
    - HIPAA: 60 days to individuals and HHS
    - Contractual obligations to partners
2. Assess affected population
    - What data was stolen?
    - How many individuals are affected?
    - What jurisdictions are involved?
    - What are harm potentials?
3. Engage notification vendor
    - Letter printing and mailing
    - Email notification services
    - Call center for questions
    - Credit monitoring offers (12-24 months typical)

Week 2-3: Execute Notifications

Regulatory Notifications:

- File required regulatory reports
- Provide incident details
- Document notification
- Respond to regulatory inquiries

Individual Notifications:

- Letter Template:

None

[DATE]

Dear [NAME],

We are writing to inform you of a data security incident that may have affected your personal information.

WHAT HAPPENED:
On [DATE], we discovered that unauthorized individuals accessed our systems and may have stolen certain data, including information related to you.

WHAT INFORMATION WAS INVOLVED:
The potentially affected information includes [SPECIFIC DATA TYPES: names, addresses, SSN, financial data, medical data, etc.].

WHAT WE ARE DOING:
We have taken the following steps:
- Immediately contained the incident
- Engaged leading cybersecurity experts to investigate
- Notified law enforcement
- Implemented enhanced security measures
- [If applicable: Chosen not to pay ransom to criminal actors]

WHAT YOU CAN DO:
We recommend you take the following precautions:
- [Specific recommendations based on data types]
- Monitor your accounts for suspicious activity
- Consider placing fraud alert or credit freeze
- [If offering: Enroll in complimentary credit monitoring service we are providing]

FOR MORE INFORMATION:
We have established a dedicated call center at [PHONE NUMBER] and website at [URL] where you can get more information and ask questions.

We sincerely apologize for this incident and any concern it may cause you.
We take the security of your information very seriously and are committed to preventing incidents like this in the future.

Sincerely,
[NAME]
[TITLE]

Media/Public Statement:

- Prepared statement for media inquiries
- FAQ for website
- Social media response plan
- Executive spokesperson designated

Managing Data Leak Aftermath

When Threat Actors Leak Data:

1. Monitor leak sites
    - Dark web monitoring services
    - Threat intelligence feeds
    - Check known ransomware leak sites daily
2. Assess leaked data
    - What was actually published?
    - Does it match what was stolen?
    - Is it searchable/accessible?
    - Can it be taken down? (Usually no)
3. Damage control
    - Supplemental notifications if needed
    - Enhanced support for affected individuals
    - Media management
    - Stakeholder communication
4. Legal action
    - Law enforcement investigation
    - Civil litigation (difficult against anonymous actors)
    - DMCA takedowns (limited effectiveness)

3A.4 Operational Workarounds During Recovery

Maintaining Business Operations Without Full Systems:

Temporary Solutions

Manual Processes:

- Paper-based order taking
- Spreadsheet tracking
- Phone-based coordination
- Manual calculations

Cloud Services:

- Quick Office 365/Google Workspace deployment
- Cloud-based CRM (Salesforce temporary)
- Cloud file storage (Dropbox, Box)
- Web-based collaboration tools

Mobile Devices:

- Work from personal devices temporarily
- Mobile hotspots
- Smartphone-based workflows
- Tablet deployments

Partner Resources:

- Leverage partner systems
- Temporary hosting arrangements
- Data processing outsourcing
- Shared infrastructure

Communication During Downtime

Internal Communication:

- Daily all-hands calls
- Status update emails (personal accounts)
- Whiteboard command centers
- Physical postings in offices

Customer Communication:

- Service status page
- Email updates (if email operational)
- Social media updates
- Phone tree for critical customers
- Website banner notices

Transparency Approach:

None

"We are currently experiencing a systems outage due to a cybersecurity incident. We are working around the clock to restore services.

Current Status:
- [SERVICE A]: Operational with delays
- [SERVICE B]: Temporarily unavailable, expected [DATE]
- [SERVICE C]: Operating normally

We appreciate your patience and will provide updates every [FREQUENCY]."

PHASE 3B: NEGOTIATION PATH (Payment)

Last Resort: Engaging with Threat Actors

WARNING: Only proceed if Recovery Path is not viable and board has authorized

3B.1 Pre-Negotiation Requirements

CRITICAL: OFAC Compliance Review

BEFORE ANY CONTACT with threat actors, complete this:

Step 1: Engage OFAC Specialist Attorney (Immediately)

- Find attorney specializing in OFAC sanctions
- Major firms: Gibson Dunn, Kirkland & Ellis, Covington & Burling
- Cost: $500-800/hour, budget $50-100K for full compliance review

Step 2: Threat Actor Identification

Sanctioned Ransomware Groups (DO NOT PAY):

- Evil Corp / Dridex gang
- Conti (and all successors/rebrands)
- DarkSide / BlackMatter
- North Korean groups (Lazarus, Bluenoroff, Andariel)
- Any group with connections to sanctioned countries (Russia, Iran, North Korea)

Resources for Screening:

- OFAC SDN List: https://sanctionssearch.ofac.treas.gov
- Chainalysis sanctions screening
- TRM Labs compliance tools
- Blockchain analysis of Bitcoin wallets

Step 3: Document Screening Efforts

Create compliance file containing:

- Screenshots of OFAC database searches
- Blockchain analysis reports
- Threat intelligence reports on ransomware group
- Attempts to determine group identity
- Legal memorandum on compliance efforts
- Date/time stamps of all searches

Why This Matters:

- Good faith compliance efforts may reduce penalties if wrong
- Required for insurance coverage
- Protects executives personally
- Demonstrates reasonable care

Step 4: Decision Point

If Sanctioned Entity Confirmed:

- STOP all negotiation immediately
- Return to Recovery Path (no choice)
- Report to OFAC
- Document decision and rationale

If Sanctioned Entity Suspected But Uncertain:

- Consider applying for OFAC license (rarely approved, takes weeks)
- Consult with OFAC attorney on risk tolerance
- Document uncertainty and decision rationale
- Consider Recovery Path instead

If Non-Sanctioned Entity Confirmed:

- Proceed with negotiation (still ethically questionable)
- Maintain ongoing monitoring (groups sometimes re-designated)
- Document clearance decision

Insurance Coordination

Required Actions:

1. Confirm coverage for ransom payment
    - Some policies exclude or sub-limit ransom
    - Understand coverage caps
    - Verify negotiation specialist coverage
    - Get written confirmation of coverage
2. Use approved vendors if required
    - Many policies require approved IR firms
    - Panel counsel may be mandatory
    - Deviation could void coverage
3. Document all costs meticulously
    - Forensics costs
    - Legal costs
    - Negotiation specialist costs
    - IT recovery costs
    - Business interruption

Establish Negotiation Infrastructure

Communication Setup:

1. Isolated Environment

- Dedicated laptop NOT connected to corporate network
- Fresh Windows installation
- Virtual machine preferred
- No corporate credentials stored

2. Tor Browser Installation

- Download from official source only: https://www.torproject.org
- Verify signature
- Test access to .onion addresses
- Understand this routes through Tor network

3. Encrypted Communication Tools

- Tox Messenger: https://tox.chat (if threat actor uses Tox ID)
- ProtonMail: Encrypted email account
- Signal: For internal team coordination
- All separate from corporate infrastructure

4. Documentation System

- Screenshot every communication
- Timestamp all messages
- Maintain negotiation log
- Store in attorney-client privileged folder

Cryptocurrency Infrastructure:

1. Exchange Account Setup (START THIS EARLY)

Timeline: 7-14 days for full setup

Day 1-2: Account Creation

- Open accounts at major exchanges:
  - Coinbase (easiest for US)
  - Kraken (good international support)
  - Gemini (institutional-friendly)
- Use corporate email and information
- Provide business registration documents

Day 3-7: Identity Verification (KYC)

- Upload corporate documents:
  - Articles of incorporation
  - EIN documentation
  - Business licenses
  - Beneficial ownership information
- Upload ID for authorized signers
- Provide proof of address
- Video verification may be required
- Response time varies by exchange

Day 7-10: Banking Integration

- Link corporate bank account
- Micro-deposit verification
- Set wire transfer instructions
- Increase purchase limits (requires business verification)

Day 10-14: Large Transaction Approval

- Request limit increase for large purchases ($500K+)
- Provide explanation for purchase (incident response)
- Compliance review by exchange
- May require additional documentation

2. Hardware Wallet Acquisition

- Ledger Nano X or Trezor Model T
- Purchase from official manufacturer only
- Test with small transactions
- Store seed phrase in physical safe
- Multiple signers if possible

3. Test Transaction

- Purchase $100-500 in Bitcoin
- Transfer to hardware wallet
- Verify can send from wallet
- Understand transaction fees and confirmation times

Budget Preparation:

Calculation:

```
None
Expected Ransom Payment (after 50% negotiation): $_____

Additional Transaction Costs:
- Exchange fees (0.5-2%): $_____
- Network transaction fees: $50-200
- Wire transfer fees: $25-50
- Price volatility buffer (5%): $_____

Total Payment Budget: $_____
```

3B.2 Initial Contact and Assessment

When to Make First Contact

Recommended Timing:

- 24-48 hours after incident detection (shows you're not panicking)
- After OFAC compliance review completed
- After backup restoration assessment completed (know your alternatives)
- After board authorization obtained
- After insurance activated

Don't Contact If:

- OFAC issues unresolved
- Free decryptor might be available (check No More Ransom)
- Backup restoration likely to succeed faster
- Volume Shadow Copies might work (check first)

First Message Strategy

Philosophy:

- Establish communication without showing desperation
- Test their responsiveness and professionalism
- Buy time for parallel recovery efforts
- Gather intelligence on their operation
- Maintain leverage

Template Message (Recommended):

None

We have received notification of an incident affecting our systems.

Before we can consider any course of action, we require verification:

1. Proof that you possess decryption capability
   Please provide decryption of the attached [3-5] sample files from different systems. We need to verify both the authenticity of this communication and your technical capability.

2. Confirmation of scope
   What systems and data are affected?

3. Verification of your identity
   Which group are we communicating with?

We are simultaneously evaluating alternative recovery methods. We will assess your response and our options before determining next steps.

Our response time will be approximately 48-72 hours as this requires internal review at multiple levels.

Why This Approach Works:

- Doesn't commit to negotiation
- Requests proof (they usually provide)
- Sets expectation of slow decision-making
- Signals you have alternatives
- Maintains control of timeline

Alternative (More Aggressive):

None

We have identified the security incident.

We are currently restoring systems from backups. This process is [X%] complete and expected to finish within [X] days.

We have not decided whether negotiation is necessary or worthwhile. If backup restoration succeeds, we will not engage further.

If you can provide business justification for negotiation (meaningful time savings
or guaranteed data deletion), provide details on:
- Exact scope of encrypted systems
- Proof of decryption capability (decrypt the attached files)
- Evidence of data in your possession
- Your best and final price

We will evaluate and respond within 72 hours.

Why This Works:

- Signals you might walk away
- Creates urgency for them (you have alternatives)
- Demands their best offer upfront
- Shows you're sophisticated buyer

Assessing Threat Actor Response

Indicators of Professional Operation:

Positive Signs:

- Prompt response (within 24 hours)
- Provides test decryption successfully
- Professional communication (minimal language errors)
- Specific details about your environment
- Reasonable negotiation stance
- Willing to wait for approvals
- Established brand (known group)

❌ Red Flags:

- No response or very delayed (>72 hours)
- Refuses or can't provide test decryption
- Generic messages (could be anyone)
- Extremely aggressive timelines
- Inconsistent information
- Changes communication channels repeatedly
- Requests unusual payment methods
- Known reputation for not providing decryptors

Test Decryption Validation:

What to Request:

- 3-5 files from DIFFERENT systems
- Mix of file types (documents, databases, images)
- Include one larger file (50-100MB) to test performance
- From systems of varying criticality

How to Validate:

- Verify files decrypt correctly
- Check file integrity (open and use them)
- Confirm matches original file (if you have sample)
- Assess decryption speed
- Document success rate

Common Issues:

- Test decryption works but full decryption fails
- Corruption during decryption process
- Extremely slow performance at scale
- Decryptor crashes on large datasets

If Test Decryption Fails:

- Request re-test with different files
- If continues to fail, strong signal to walk away
- Document failures for decision-making
- Consider returning to Recovery Path

Gathering Intelligence

Information to Extract:

About Their Operation:

- Which ransomware family/group are they?
- Do they have an existing leak site? (check)
- What's their history/reputation? (research on forums)
- Have they been sanctioned?
- What's their typical negotiation range?

About Your Compromise:

- How long did they have access? (dwell time)
- What was the initial access vector?
- What data do they actually have? (specifics)
- How much data was exfiltrated? (GB/TB)
- Which systems are encrypted?

About Their Demands:

- Initial ransom amount
- Deadline pressure (real or artificial?)
- Payment method (Bitcoin, Monero, etc.)
- Negotiation willingness
- Leak threats (timing, platform)

3B.3 Advanced Negotiation Tactics

The Negotiation Mindset

Key Principles:

1. This is a business transaction with criminals
    - They want money with minimum effort
    - You want decryption with minimum payment
    - Both sides have incentives to conclude deal
    - But they have more experience than you
2. Time is your friend, not your enemy
    - Don't rush despite their artificial deadlines
    - Longer negotiation = better discount typically
    - Parallel recovery efforts improve your leverage
    - They're juggling many victims, you're their customer
3. Information asymmetry is leverage
    - They don't know your financial situation
    - They don't know your insurance limits
    - They don't know if backups work
    - They don't know your desperation level
    - Maintain mystery on all these points
4. Their "deadlines" are almost always fake
    - Leak deadlines get extended regularly
    - Encryption doesn't degrade (they can decrypt anytime)
    - They want payment, walking away helps nobody
    - Exception: If they leak, it's usually over

Negotiation Strategy Framework

Round 1: The Anchor (Days 1-3)

Their Opening: $5,000,000

Your Response Strategy: Start at 10-15% of demand

None

We have completed initial assessment of the situation.

Our organization's total available budget for any incident response, including potential ransomware payment, is limited to $500,000. This is a hard constraint based on insurance policy limits and organizational resources.

We are simultaneously pursuing backup restoration, which is showing promise.
Whether we proceed with any payment depends entirely on:
1. Meaningful time savings vs. backup restoration
2. Verified guarantee of data deletion
3. Agreement within our budget constraints

If you can work within this budget, we can discuss next steps. If not, we will proceed with our restoration efforts.

Response timeframe: We will evaluate your response and provide decision within 72 hours.

Why This Works:

- Anchors at your low number, not their high number
- Provides justification (insurance limits) for low offer
- Creates competition (backup restoration)
- Sets expectation of slow decision process
- Gives them option to significantly reduce or walk away

Expected Response:

- Rejection of your low offer
- Counter-offer at 60-80% of original ($3M-4M)
- Pressure tactics about data leak
- Artificial deadline imposition

Round 2: Manufactured Obstacles (Days 4-6)

Their Counter: $3,500,000

Your Response Strategy: Minimal movement + introduce external gatekeepers

None

We have reviewed your response with our insurance carrier and legal counsel.

Several significant obstacles have emerged:

1. Insurance Limitations
   Our carrier will only approve coverage up to $800,000 for ransomware payments. We cannot exceed this without voiding our policy.

2. OFAC Compliance Review
   Our legal counsel requires 5-7 days to complete sanctions screening before any payment authorization. This is non-negotiable for legal compliance.

3. Board Approval Required
   Any payment over $500K requires board approval, which requires:
   - Comprehensive cost-benefit analysis
   - Proof of decryption capability beyond test files
   - Legal opinion on compliance
   - Board meeting (next scheduled in 5 days)

4. Backup Restoration Progress
   Our restoration efforts are now 40% complete. If we reach 60% completion, cost-benefit analysis will favor completion of restoration over payment.

For us to proceed with negotiation track (vs. restoration track), we would need:
- Agreement in principle on payment in the $800K range
- Additional proof of decryption capability (full small server, not just files)
- Binding commitment on data deletion with verification method
- Minimum 10-day timeline for all approvals

Please advise if these parameters are workable. Otherwise, we will focus resources on restoration completion.

Why This Works:

- Creates external obstacles (insurance, legal, board) vs. your stubbornness
- Introduces time delays that favor you
- Shows minimal movement (10% → 16%)
- Maintains competitive pressure (restoration progress)
- Requests additional proof (reasonable)
- Makes them work to keep you engaged

Expected Response:

- Frustration at slow pace
- Pressure about data leak
- Counter-offer at 40-50% of original ($2M-2.5M)
- May provide additional decryption proof
- May extend "deadline"

Round 3: The Insurance Maximum Gambit (Days 7-10)

Their Counter: $2,000,000

Your Response Strategy: The "highest I can go" limit

None

Following extensive internal discussions and insurance carrier negotiation,
I can present the following final position:

MAXIMUM APPROVED PAYMENT: $1,200,000

This represents:
- Our insurance policy maximum for ransomware coverage
- Board-approved emergency expenditure limit
- Absolute ceiling of available funds

To proceed at this amount, we require:

TECHNICAL VERIFICATION:
- Successful decryption of complete test server (500GB-1TB)
- Demonstrated decryption speed and estimated completion time
- Decryptor compatibility with our environment verified
- Written technical documentation for decryption process

LEGAL PROTECTIONS:
- Confirmation you are not a sanctioned entity (we will verify)
- Written commitment to:
  * Delete all stolen data immediately upon payment
  * Provide proof of deletion (method to be agreed)
  * Not release data to third parties
  * Not re-attack our organization for 12 months minimum

PAYMENT TERMS:
- Payment in Bitcoin to single wallet address (verified through two channels)
- Decryptor provided upon payment confirmation
- Payment timeline: 24-48 hours after all conditions met

THIS IS OUR FINAL POSITION. Amounts above $1.2M are literally not available to us.

If you cannot agree to these terms, we will complete backup restoration (currently 65% complete) and accept the data leak risk.

Please confirm acceptance or provide your absolute minimum. We need response within 72 hours to maintain negotiation track vs. restoration completion.

Why This Works:

- Claims "final position" (they expect this)
- Arrives at 20-25% of original demand (typical successful range)
- Creates urgency for THEM (you might walk away)
- Detailed requirements show sophistication
- "12 month commitment" is unenforceable but sounds good
- Sets stage for closing

Expected Response:

- Counter somewhere between $1.2M-1.5M
- Or acceptance of $1.2M (success)
- Or ultimatum at higher number (call bluff)

Round 4: Final Negotiation (Days 10-14)

Their Counter: $1,500,000 "final offer"

Your Response: Hold firm or minor movement

Option A: Hold Firm

None

We have reviewed your response. Unfortunately, $1,500,000 exceeds our organizational capability.

$1,200,000 remains our maximum available payment. This is not a negotiating position - it is a financial reality.

We have two paths forward:
1. Agreement at $1,200,000 with immediate payment execution
2. We complete backup restoration (now 75% complete, 5-7 days to operational)

The decision is yours. We are prepared for either outcome.

Option B: Split the Difference (if must)

None
Final offer: $1,350,000

This requires us to:
- Reduce other incident response expenditures
- Defer planned security improvements
- Accept budget shortfall in other areas

This is absolutely our maximum. Agreement at this number enables immediate payment execution. Any higher amount is not feasible and we will complete restoration instead.

Please confirm acceptance within 24 hours.

Alternative Negotiation Tactics

Tactic 1: Staged Payment

When stuck at impasse, offer split payment:

None
Proposal: Staged Payment Structure

Phase 1: $700,000 upon receipt and verification of decryption key
- You provide decryptor immediately
- We begin decryption of critical systems
- Verify decryptor functionality at scale

Phase 2: $500,000 upon successful decryption of 50%+ of systems (5-7 days)
- Confirms decryptor works fully
- Reduces our risk of non-functional decryptor
- You receive full payment once proven

Total: $1,200,000 (our maximum)
Benefits for you: Demonstrates good faith, faster initial payment
Benefits for us: Risk mitigation

Success Rate: ~30% of sophisticated groups accept this

Tactic 2: The Competitive Bid

When free decryptor already exist or a research is ongoing:

None

We have been contacted by [security research firm] who claims to have decryption method for [ransomware family] due to cryptographic vulnerability they discovered.

They are offering decryption services for $400,000.

We are evaluating their approach over next 48 hours.

If you can match or beat that price, we would prefer to work with you directly as you have the authoritative decryption key.

Otherwise, we will pursue the research-based approach.

Warning: Only use if there's actually research into that ransomware family. They'll verify.

Tactic 3: The Regulatory Forced Hand

Create artificial urgency that benefits you:

None

UPDATE: Regulatory Complication

Our legal counsel has advised that under [GDPR/HIPAA/etc.], we are required to notify regulators and affected individuals within 72 hours of confirming data breach.

We are now at hour 60.

Once notification occurs:
- Incident becomes public record
- Law enforcement intensifies involvement
- Payment becomes more legally complicated
- Our window for confidential resolution closes

We can authorize immediate payment of $1,100,000 and complete transaction within 12 hours to avoid notification deadline.

Above this amount requires additional approvals that push past deadline, forcing public notification.

You have until [SPECIFIC TIME] to accept. After that, notification triggers and opportunity closes.

Why This Works: Creates real urgency for threat actor, not you

Pressure Tactics and Counter-Tactics

Their Tactic: Data Leak Threat

"We will begin leaking your data in 24 hours unless payment is received."

Your Counter:

None

We understand you have data exfiltration capability.

However, leaking data will:
1. Eliminate any possibility of payment (triggers mandatory law enforcement reporting)
2. Destroy your reputation in criminal ecosystem (bad for business)
3. Provide law enforcement extensive evidence for investigation
4. Remove your leverage entirely

We are negotiating in good faith within our financial constraints. Leaking serves neither party's interests.

Our position remains $1,200,000. We can execute payment within 48 hours if agreed. Otherwise, we proceed with backup restoration.

Threats do not create money that doesn't exist.

Their Tactic: Artificial Deadline

"Price increases to $10M in 24 hours."

Your Counter:

None

Artificial deadline changes do not affect our financial reality or approval processes.

We are moving as quickly as organizational governance allows. Board approval requires specific timeline. Insurance authorization requires documentation.

Adding pressure does not accelerate approvals or create additional budget.

We can pay $1,200,000 on [DATE] following proper approvals, or we can pay nothing and complete restoration.

The decision is yours. Choose the timeline: payment on our approval schedule, or no payment and we restore.

Their Tactic: Partial Data Leak

"Here is a sample of your data on our leak site. More released daily unless paid."

Your Counter:

None
We acknowledge the data publication.

This does not change our financial constraints or authorization limits.

Our position remains $1,200,000 maximum available. Further leaks do not create additional budget.

You can:
1. Accept $1,200,000 and receive payment
2. Continue leaking and receive nothing

Continuing to leak while negotiating is counterproductive. We are authorized to pay within our limits. We are not authorized to pay beyond them.

Your decision whether to accept payment that's available.

Their Tactic: Multiple Attackers Claim

"We have sold your data to other groups who will attack you."

Your Counter:

None
If true, this significantly reduces the value of any agreement with you.

Our willingness to pay was contingent on data protection. If data is already distributed, payment provides no benefit.

Either:
1. This claim is false and we can proceed with negotiation
2. This claim is true and negotiation is pointless

Please clarify.

What NOT to Do in Negotiation

⊗ Don't Show Desperation

- "We need systems back immediately"
- "Our business is dying"
- "Customers are leaving" → This increases their price demands

⊗ Don't Reveal True Financial Capacity

- "We have $5M in insurance"
- "Board approved up to $3M"
- "We can access credit line" → They will demand that amount

⊗ Don't Threaten Law Enforcement

- "We're reporting you to FBI"
- "Interpol is investigating"
- "You'll be caught" → They don't care and it's counterproductive

⊗ Don't Make Personal Attacks

- "You're criminals"
- "This is unethical"
- "You're scum" → Business-like tone works better

⊗ Don't Accept First Offer

- They expect negotiation
- First offer is intentionally high
- You leave money on table

⊗ Don't Move Too Quickly

- Each concession should take days
- Instant response signals desperation
- Slow pace is your friend

⊗ Don't Pay Without Test Decryption

- Some groups can't decrypt
- Some decryptors are broken
- Verify before payment

⊗ Don't Trust Promises About Data Deletion

- Verification is impossible
- They can keep copies
- They may have already sold data
- "Agreement" is meaningless

3B.4 Payment Execution

Pre-Payment Final Verification

Complete Before Any Payment.

Technical Verification:

- Test decryption successful on sample files
- Test decryption successful on full test server (if possible)
- Decryptor performance acceptable
- Decryption time estimate reasonable
- Technical documentation provided
- Support contact information confirmed

Legal Verification:

- OFAC compliance review completed and documented
- Legal counsel approved payment
- Board authorization obtained (with documented vote)
- Insurance carrier notified of impending payment
- Payment authorization signatures obtained
- All decision rationale documented

Financial Verification:

- Cryptocurrency exchange account funded
- Bitcoin purchased (or ready to purchase at current rate)
- Hardware wallet configured and tested
- Wallet address verified through two separate channels
- Transaction fees budgeted
- Payment timeline agreed with threat actor

Operational Verification:

- Incident response team ready for decryption
- Parallel backup restoration ready (if payment fails)
- Communication plan for post-payment
- Monitoring for decryptor delivery
- Escalation plan if issues arise

Bitcoin Payment Process

Step 1: Final Wallet Address Verification (CRITICAL)

The Problem: Typosquatting attacks and man-in-the-middle attacks can cause you to send millions to the wrong address.

Verification Process:

1. Get address through primary channel (Tor chat, email)
2. Request verification through DIFFERENT channel (if available - different email, different Tor session)
3. Compare addresses character by character (use multiple people)
4. Check address hasn't been reported as scam (bitcoinabuse.com, whale-alert.io)
5. Send small test transaction first ($1,000-$5,000)
6. Get confirmation from threat actor before sending remainder
7. Wait for blockchain confirmation (typically 10-30 minutes for 1 confirmation)

Document Everything:

- Screenshot of address provided
- Screenshot of verification through second channel
- Timestamp of verification
- Names of people who verified
- Store in legal hold folder

Step 2: Bitcoin Purchase

Option A: Pre-Purchase (Lower Risk)

- Purchase Bitcoin days before payment needed
- Store in hardware wallet
- Avoids price volatility during crisis
- Reduces payment day complexity
- Risk: Bitcoin price drops (you lose value)

Option B: Purchase at Payment Time (Standard)

- Purchase Bitcoin immediately before payment
- Current market rate
- Transfer directly to payment
- Risk: Price volatility during purchase and transfer

Purchase Process:

1. Wire transfer to exchange (if not already funded)
    - Same-day wire from bank
    - Usually arrives in 2-4 hours
    - Confirm receipt before proceeding
2. Purchase Bitcoin
    - Use market order for immediate execution (vs. limit order)
    - Purchase amount: (Ransom + 5% buffer for fees/volatility)
    - Confirm purchase completion
    - Note: Exact BTC amount, USD amount, exchange rate
3. Transfer to hardware wallet (if using)
    - Send from exchange to your wallet
    - Wait for confirmation (30-60 minutes)
    - Verify receipt in wallet

Step 3: Payment Transaction

Final Pre-Payment Checklist:

- Wallet address verified (multiple methods)
- Bitcoin amount calculated (account for any price movement)
- Exchange rate locked with threat actor (if using specific USD amount)
- Transaction fee set appropriately (higher fee = faster confirmation)
- All stakeholders informed (CEO, CFO, legal, board)
- Documentation systems ready (screenshots)
- Incident response team on standby
- Threat actor confirmed ready to deliver decryptor

Execute Payment:

1. Initiate Transfer

```
None
From: Your wallet
To: [Verified threat actor wallet address]
Amount: [X.XXXXX] BTC
Fee: [Standard/Priority/Urgent]
```

2. Confirm Transaction Details
    - Review wallet address one final time
    - Review Bitcoin amount
    - Confirm fee is appropriate
    - Take screenshot
3. Broadcast Transaction
    - Click send/confirm
    - Transaction now on blockchain
    - Cannot be reversed
4. Document Transaction
    - Transaction ID (TXID) - copy immediately
    - Blockchain explorer link
    - Screenshot of transaction
    - Timestamp
    - Confirmation of broadcast
5. Monitor Confirmation
    - Watch blockchain explorer (blockchain.com, blockchair.com)
    - First confirmation: typically 10-60 minutes
    - Most groups accept 1 confirmation
    - Some require 3-6 confirmations (up to 1 hour)

6. Notify Threat Actor

None

Payment has been sent.

Transaction ID: [TXID]
Amount: [X.XXXXX] BTC
Blockchain explorer: [LINK]

Confirmations: [X]/[Required]

Please confirm receipt and provide decryption key.

Step 4: Decryptor Delivery

Expected Timeline:

- Immediate to 4 hours after payment confirmation
- Most professional groups: within 1 hour
- Some require multiple confirmations first

Delivery Methods:

- Download link (Tor .onion site)
- File upload to chat platform
- Direct message with attached file
- Sometimes delivered before full confirmations

Upon Receipt:

1. Do NOT run immediately on production
    - Download to isolated system
    - Scan with antivirus (may detect as malware - normal)
    - Test on isolated virtual machine first
2. Verify Decryptor
    - Matches description provided
    - File hashes match (if provided)
    - Documentation included
    - Support contact information
3. Test on Non-Critical System First
    - Choose small, non-critical system
    - Full decryption test
    - Verify file integrity
    - Assess performance
    - Document any issues

4. If Decryptor Fails

None

Decryptor testing has identified issues:

[Specific technical problems]

We need:
- Corrected decryptor version, or
- Technical support to resolve issues, or
- Partial refund if decryption not possible

Please respond within 24 hours.

If Threat Actor Doesn't Deliver:

Hour 1-4: Wait patiently (they're often busy)

Hour 4-8: Send reminder

None

Payment confirmed with [X] confirmations.

Transaction: [TXID]

Awaiting decryptor delivery as agreed.

Please confirm status.

Hour 8-24: Escalate

None

Payment of [X] BTC completed over [X] hours ago.

No decryptor received.

This represents breach of agreement. Please deliver decryptor immediately or confirm issue preventing delivery.

If no response within 24 hours, we will proceed with backup restoration and report breach to law enforcement and industry forums.

After 24 hours:

- Accept loss (unfortunately common ~10-15% of cases)
- Proceed with backup restoration
- Report to FBI and insurance
- Report to ransomware tracking sites (BleepingComputer forum)
- Document for legal proceedings
- Warn other organizations (if appropriate)

Post-Payment Communication

Document Everything:

- Complete negotiation transcript
- Payment proof (blockchain transaction)
- Decryptor delivery confirmation
- All communications saved
- Timeline documented

Stakeholder Notifications:

Internal:

- "Payment completed, decryptor received, beginning decryption process"
- Expected timeline to restoration
- Risks and contingencies

Insurance:

- Payment confirmation with documentation
- Decryptor received
- Claim continuation for recovery costs

Law Enforcement:

- Payment details (TXID, amount, wallet address)
- Complete communication logs
- Decryptor sample (for their analysis)
- Attribution information

DO NOT Announce Publicly:

- Payment details
- Ransom amount
- That you paid at all (if possible)
- Negotiation details

3B.5 Decryption and Recovery

Decryption Execution Strategy

Phase 1: Controlled Pilot (Days 1-2)

Select Pilot Systems:

- 2-3 non-critical servers
- Different system types (Windows, Linux)
- Varying data sizes (small, medium, large)
- Different encryption completeness levels

Pilot Objectives:

- Validate decryptor functionality
- Measure decryption speed
- Identify issues early
- Estimate full timeline
- Develop procedures

Pilot Process:

1. Isolate pilot systems
    - Separate network segment
    - No connectivity to production
    - Monitoring enabled
2. Run decryptor
    - Document exact steps
    - Record start time
    - Monitor progress
    - Note any errors
    - Capture logs
3. Validate results
    - Files decrypt correctly?
    - Data integrity maintained?
    - Applications function?
    - Performance acceptable?
4. Calculate estimates
    - Decryption speed: X GB per hour
    - Total data encrypted: Y TB
    - Estimated completion: Y TB / X GB = hours
    - Add 20-30% buffer for issues

Phase 2: Staged Production Decryption (Days 2-14)

Prioritization (Same as Backup Restoration):

Tier 1: Critical Business Systems

- Production databases
- Customer-facing applications
- Email systems
- Financial systems
- Target: Days 2-5

Tier 2: Supporting Systems

- File servers
- Internal applications
- Collaboration tools
- Target: Days 5-10

Tier 3: Lower Priority

- Archive data
- Development systems
- Non-essential systems
- Target: Days 10-14+

Execution Approach:

Option A: Parallel Decryption

- Run decryptor on multiple systems simultaneously
- Faster overall completion
- Higher resource usage
- More complexity
- Risk: Issues multiply

Option B: Sequential Decryption

- Decrypt one system at a time
- Slower overall
- Lower resource usage
- Easier troubleshooting
- Safer approach

Recommended: Hybrid

- Decrypt 3-5 systems in parallel
- Focus on same-tier systems
- Monitor closely
- Pause if issues emerge

Decryption Monitoring:

- Dedicated monitoring team
- Progress tracking dashboard
- Issue escalation process
- Regular status updates
- Expected completion timeline

Common Decryption Problems

Problem 1: Decryptor Crashes/Hangs

Symptoms:

- Process stops responding
- No progress for extended period
- Error messages
- System resource exhaustion

Solutions:

- Restart decryptor (usually safe)
- Run on system with more resources
- Decrypt in smaller batches
- Contact threat actor for support (if available)
- May need to decrypt files individually

Problem 2: Partial Decryption

Symptoms:

- Some files decrypt, others don't
- Certain file types skip
- Specific directories not processed

Solutions:

- Run decryptor multiple times
- Use different decryptor flags/options (if available)
- Manual file recovery for important files
- Contact threat actor for updated decryptor
- Accept data loss on non-critical files

Problem 3: File Corruption

Symptoms:

- Files decrypt but won't open
- Data appears corrupted
- Applications crash on files
- Databases won't load

Causes:

- Original encryption was imperfect
- Decryptor has bugs
- Storage issues during encryption
- File system corruption

Solutions:

- Try file repair tools
- Restore from backup if available (hybrid approach)
- Database recovery procedures
- May require manual reconstruction

Problem 4: Extremely Slow Performance

Symptoms:

- Decryption taking 10x longer than estimated
- TB of data requiring weeks
- System resources maxed out

Reality Check:

- Some decryptors are genuinely slow
- Encryption is CPU-intensive
- Large databases particularly slow
- May be faster to restore from backup

Solutions:

- Run on more powerful hardware
- Use GPU acceleration (if supported)
- Parallel decryption on multiple machines
- Consider hybrid: decrypt critical, restore rest from backup

Problem 5: Reinfection During Decryption

Symptoms:

- Files re-encrypt during decryption
- New encryption events occur
- Systems compromised again

Critical Problem: Initial Access Vector Not Eliminated

Immediate Actions:

- Stop all decryption
- Immediate containment
- Full forensic review
- Find and close access vector
- May need complete rebuild instead

Decryption Success Criteria

System Operational:

- Server boots successfully
- Services start correctly
- Applications function
- User access works
- Performance acceptable

Data Integrity:

- Critical files accessible
- Databases load correctly
- Applications can read data
- Sample validation passed
- User testing completed

Completeness:

- All expected files present
- No significant gaps
- Acceptable data loss level
-Documentation updated

When Decryption Fails:

If decryptor doesn't work or works poorly:

1. Attempt remediation with threat actor
    - Report specific issues
    - Request updated decryptor
    - Most professional groups will help
    - Set 48-hour deadline for response
2. If no resolution:
    - Accept payment loss (document for insurance)
    - Proceed with backup restoration
    - Hybrid approach: decrypt what works, restore rest
    - Document for law enforcement report
3. Legal options:
    - Insurance claim for failed ransom payment
    - Report to FBI for investigation
    - Unlikely to recover payment
    - May help other organizations

Reality: ~10-15% of ransoms result in non-functional or inadequate decryptors. This is the risk of the payment path.

PHASE 4: POST-INCIDENT ACTIVITIES (Applies to Both Recovery and Payment Paths)

This phase applies regardless of whether you paid ransom or recovered independently.

4.1 Comprehensive Forensic Investigation

Timeline: Parallel to recovery, continuing weeks after

Critical Investigation Questions

1. Initial Access Vector (MOST IMPORTANT)

How did they get in originally?

Common Vectors (Prioritized Investigation):

Remote Desktop Protocol (RDP) Compromise:

- Evidence: Windows Event Log 4624 (logon) from external IP
- Check: Internet-facing RDP ports (3389)
- Review: Failed login attempts (Event 4625) before success
- Common issue: Weak passwords, no MFA

VPN Appliance Exploitation:

- Evidence: VPN logs showing unusual authentication
- Check: Unpatched VPN devices (FortiGate, Pulse Secure, Cisco)
- Review: CVE history for your VPN device
- Common issue: Known vulnerabilities, credential stuffing

Phishing/Credential Theft:

- Evidence: Email delivery to user, followed by credential use
- Check: Email gateway logs, user reports, browser history
- Review: Suspicious links, malicious attachments
- Common issue: Spearphishing, credential harvesting sites

Supply Chain/Third-Party Access:

- Evidence: Compromise came through MSP or vendor credentials
- Check: Third-party access logs, privileged accounts
- Review: MSP security practices
- Common issue: Weak MSP security, over-privileged access

Software Vulnerability:

- Evidence: Web server logs showing exploitation attempts
- Check: Public-facing applications, unpatched systems
- Review: Vulnerability scan results
- Common issue: Unpatched critical vulnerabilities

Investigation Process:

1. Timeline Construction
    - First evidence of attacker presence
    - Key attacker actions chronologically
    - Encryption event timing
    - Identify patient zero system
2. Log Analysis
    - Windows Event Logs (Security, System, Application)
    - Firewall logs (inbound/outbound connections)
    - VPN authentication logs
    - DNS query logs
    - Email gateway logs
    - EDR/antivirus logs
    - Application logs
3. Artifact Collection
    - Malware samples (tools used by attacker)
    - Registry changes
    - Scheduled tasks/services created
    - User account creations
    - Group policy modifications

2. Dwell Time - How Long Were They Inside?

Evidence Sources:

- First observed attacker activity (logs)
- File creation timestamps (attacker tools)
- Lateral movement timeline
- Data staging events (before exfiltration)

Why This Matters:

- Longer dwell time = more comprehensive compromise
- Indicates sophistication and patience
- Affects trust in "cleaned" systems
- May require more aggressive remediation (complete rebuild vs. targeted)

Typical Dwell Times:

- Opportunistic attacks: Days to weeks
- Targeted attacks: Weeks to months
- APT-style ransomware: Months (very concerning)

3. Lateral Movement - How Did They Spread?

Techniques to Identify:

- Pass-the-hash attacks (using stolen NTLM hashes)
- Pass-the-ticket (Kerberos ticket theft)
- RDP lateral movement
- PSExec or similar remote execution
- WMI (Windows Management Instrumentation)
- PowerShell remoting

Investigation:

- Review authentication logs across all systems
- Identify admin credential usage patterns
- Map attacker movement path through network
- Identify compromised privileged accounts

4. Persistence Mechanisms - How Can They Return?

Common Persistence Methods:

User Accounts:

- Hidden administrative accounts
- Backdoor user accounts
- Compromised legitimate accounts
- Service accounts with persistent access

Scheduled Tasks/Services:

- Malicious scheduled tasks
- New Windows services
- Autorun registry keys
- Startup folder modifications

Remote Access Tools:

- Legitimate tools used maliciously (TeamViewer, AnyDesk, Atera)
- Custom remote access trojans (RATs)
- Web shells on public-facing servers
- VPN accounts created

Investigation:

- Audit all local administrator accounts (every system)
- Review all domain administrative groups
- Check scheduled tasks on servers
- Review services on servers
- Audit VPN accounts
- Scan for web shells
- Review third-party remote access tools

5. Data Exfiltration - What Did They Steal?

Exfiltration Methods:

- Direct internet uploads (HTTP/HTTPS)
- Cloud storage (Mega, RapidShare, Dropbox)
- FTP/SFTP transfers
- Tor hidden services
- DNS tunneling (rare)
- Email exfiltration (very rare)

Investigation:

- Review outbound firewall logs (large data transfers)
- Check DLP alerts
- Review proxy logs
- Analyze cloud access security broker (CASB) logs
- Review EDR network connections
- Bandwidth utilization analysis

Indicators:

- Large outbound transfers to unknown IPs
- Unusual off-hours network activity
- Compression/archiving activity before transfer
- Cloud storage tool usage (Rclone, MegaSync)

Forensic Deliverables

Investigation Report Should Include:

1. Executive Summary
    - Incident timeline
    - Initial access vector (how they got in)
    - Attacker actions (what they did)
    - Data exfiltration assessment
    - Persistence mechanisms found
    - Remediation recommendations
2. Technical Analysis
    - Detailed timeline with evidence
    - IOCs (Indicators of Compromise):
        - IP addresses
        - Domain names
        - File hashes
        - Registry keys
        - User accounts
    - Malware analysis
    - Attack techniques (MITRE ATT&CK mapping)
3. Root Cause Analysis
    - Vulnerability or weakness exploited
    - Why it existed (process failure, resource constraint, etc.)
    - Contributing factors
    - Lessons learned
4. Remediation Roadmap
    - Immediate actions (close initial access vector)
    - Short-term improvements (30-90 days)
    - Long-term enhancements (6-12 months)
    - Investment requirements
    - Risk reduction estimates

4.2 Complete Remediation Plan

Goal: Ensure attackers cannot return

Immediate Actions (Complete Before Restoration Finishes)

Credential Reset (Complete)

Phase 1: Emergency Admin Accounts

- Create new emergency admin accounts
- Disable ALL existing admin accounts
- New accounts with complex passwords + MFA
- Document new credentials securely

Phase 2: Privileged Account Reset

- Reset ALL domain admin passwords
- Reset ALL local admin passwords (every system)
- Reset ALL service account passwords
- Reset ALL database admin passwords
- Reset ALL network device passwords
- Reset ALL cloud admin passwords

Phase 3: User Account Reset

- Force password reset for ALL users
- Minimum 14 characters, complexity required
- Cannot reuse last 24 passwords
- Implement MFA for all external access

Phase 4: API Keys and Tokens

- Regenerate ALL API keys
- Invalidate ALL access tokens
- Rotate ALL application secrets
- Update ALL integration credentials

Disable and Remove Threat Actor Access

- Delete all unauthorized user accounts
- Remove all unauthorized scheduled tasks
- Remove all unauthorized services
- Delete all unauthorized files/tools
- Remove web shells from public servers
- Disable unauthorized remote access tools
- Revoke all third-party access (re-grant as needed)
- Reset VPN devices to factory, reconfigure
- Audit and lock down all network access

Eliminate Initial Access Vector

Based on forensic findings, take specific action:

If RDP Compromise:

- Disable RDP on all systems exposed to internet
- Require VPN for any remote access
- Implement Network Level Authentication (NLA)
- Deploy MFA for all RDP sessions
- Restrict RDP to jump boxes only
- Monitor RDP connections with alerting

If VPN Exploitation:

- Emergency patch VPN appliances
- Implement MFA for VPN (if not present)
- Restrict VPN access by IP if possible
- Deploy new VPN appliance if too old
- Review VPN logs for other compromises
- Implement certificate-based VPN authentication

If Phishing:

- Enhanced email filtering rules
- Block executable attachments (.exe, .scr, .js, .vbs, .ps1)
- Implement DMARC, SPF, DKIM
- Deploy advanced threat protection (ATP)
- Mandatory security awareness training
- Phishing simulation program

If Software Vulnerability:

- Emergency patching of exploited software
- Virtual patching at WAF if can't patch
- Remove vulnerable software if not needed
- Network segmentation to limit exposure
- Implement vulnerability management program

If Third-Party/MSP:

- Revoke all third-party access
- Review all third-party security
- Implement just-in-time access for vendors
- MFA required for all third-party access
- Session monitoring for third-party access
- Consider terminating relationship if security inadequate

Network Segmentation Improvements

Implement/Enhance Segmentation:

Segment 1: Critical Production

- Production databases
- Application servers
- Strict firewall rules
- Deny-by-default access
- MFA for all access
- Heavy monitoring

Segment 2: Corporate Users

- Workstations
- Standard office applications
- Internet access (restricted)
- Can't access Segment 1 directly

Segment 3: DMZ/Public-Facing

- Web servers
- Email gateways
- No internal network access
- Heavy hardening

Segment 4: Management

- Jump boxes
- Administrative tools
- PAM solutions
- Only for admin access

Segment 5: Guest/BYOD

- Guest WiFi
- Contractor devices
- Internet-only access
- No internal access

Micro-Segmentation:

- Segment critical servers individually
- Application-level firewalling
- Zero-trust network access (ZTNA)

Endpoint Protection Enhancement

Deploy/Enhance EDR:

- EDR on 100% of endpoints and servers
- Ransomware behavioral detection enabled
- Automatic isolation enabled
- 24/7 monitoring (SOC or MDR service)
- Response playbooks configured

Application Whitelisting (Critical):

- Deploy on ALL servers
- Only approved applications can execute
- Prevents ransomware executable launch
- Microsoft AppLocker or third-party

Patch Management:

- Automated patch deployment
- Critical patches within 72 hours
- Monthly patching cycle minimum
- Emergency patching process

Email Security:

- Advanced threat protection (ATP)
- Sandbox suspicious attachments
- Block executable attachments
- Link scanning/rewriting
- User reporting tools (phishing button)

Backup Architecture Overhaul

Implement 3-2-1-1-0 Rule (If Not Already):

3 Copies:

- Production data
- Primary backup
- Secondary backup

2 Different Media:

- Disk-based backups
- Tape or cloud

1 Offsite:

- Separate location
- Cloud storage
- Physical tape offsite

1 Offline/Immutable:

- Air-gapped tape library
- Immutable cloud storage (Object Lock)
- Physical disconnection from network

0 Errors:

- Automated validation
- Test restores monthly
- Integrity monitoring

Additional Requirements:

- Separate administrative domain for backups
- MFA for backup system access
- Backup monitoring with alerting
- Quarterly full disaster recovery test
- Backup stored on separate network segment
- Backup data encrypted at rest
- Document restoration procedures

Privileged Access Management (PAM)

Implement PAM Solution:

Capabilities Required:

- Password vaulting (no more shared passwords)
- Just-in-time access (no standing privileges)
- Session recording (audit all privileged access)
- Automatic password rotation
- Approval workflows for sensitive access
- Emergency break-glass procedures

Leading Solutions:

- CyberArk
- BeyondTrust
- Delinea (Thycotic)
- Microsoft Defender for Identity

Implementation:

- Phase 1: Domain admin accounts
- Phase 2: Server local admins
- Phase 3: Database admins
- Phase 4: Network device admins
- Phase 5: Cloud admins
- Phase 6: Application admins

Multi-Factor Authentication (MFA) Everywhere

MFA Required On:

- VPN access
- RDP/SSH access
- Email (Office 365, Gmail)
- All SaaS applications
- Cloud management consoles (AWS, Azure, GCP)
- Administrative portals
- Backup systems
- Network device management

MFA Method Hierarchy (Most to Least Secure):

1. FIDO2 hardware keys (YubiKey, Titan)
2. Microsoft Authenticator (push notifications)
3. Google Authenticator (TOTP codes)
4. SMS codes (least secure, but better than nothing)

Conditional Access Policies:

- Require MFA from outside corporate network
- Require MFA for all administrative access
- Require MFA for sensitive applications
- Block legacy authentication protocols

Detection and Response Capability

SIEM Implementation/Enhancement:

Log Sources to Include:

- Windows Event Logs (all systems)
- Linux syslogs
- Firewall logs
- VPN logs
- DNS logs
- Cloud service logs (AWS CloudTrail, Azure Activity)
- EDR telemetry
- Email gateway logs
- Web proxy logs
- Database audit logs

Critical Detection Rules:

Failed Authentication:

- 10+ failed logins in 30 minutes
- Failed logins to disabled accounts
- Failed logins to admin accounts
- Alert: High

Lateral Movement:

- Admin logons from workstations
- Off-hours admin activity
- Unusual authentication patterns
- Alert: Critical priority

Ransomware Indicators:

- Mass file modifications
- File extension changes
- Backup deletion attempts
- Volume Shadow Copy deletion
- Alert: Critical priority, auto-isolate

Data Exfiltration:

- Large outbound data transfers
- Unusual cloud storage usage
- Off-hours large transfers
- Alert: High priority

Persistence:

- New scheduled task creation
- New service installation
- New user account creation
- Web shell detection
- Alert: High priority

24/7 Monitoring:

- Outsource to MSSP/MDR if no internal SOC
- Clear escalation procedures
- Response playbooks
- Regular testing

Security Awareness Program

Mandatory Training:

- ➢ Security awareness training for ALL employees
- ➢ Specific ransomware training
- ➢ Phishing recognition training
- ➢ Incident reporting procedures
- ➢ Quarterly refresher training

Phishing Simulation:

- ➢ Monthly simulated phishing campaigns
- ➢ Track click rates and reporting rates
- ➢ Remedial training for repeat clickers
- ➢ Positive reinforcement for reporters

Culture Building:

- ➢ "See something, say something" culture
- ➢ No punishment for reported mistakes
- ➢ Recognition for security-conscious behavior
- ➢ Executive leadership modeling good security

4.3 Stakeholder Communication & Regulatory Compliance

Regulatory Notification Completion

Ensure All Required Notifications Made:

GDPR (EU) - If Applicable:

Supervisory authority notified within 72 hours
Individuals notified without undue delay
Documentation maintained:

- Nature of breach
- Categories and approximate number of individuals affected
- Categories and approximate number of records affected
- Likely consequences
- Measures taken/proposed to address breach

HIPAA (Healthcare) - If Applicable:

- HHS notified (within 60 days)
- Affected individuals notified (within 60 days)
- Media notification (if >500 individuals in state)
- Business associates notified

State Breach Notification Laws (US):

- Identify all applicable states
- Review specific requirements by state
- Timing varies (typically 30-90 days)
-Attorney general notification (some states)
-Credit bureaus (some states, if large breach)

SEC (Public Companies):

- Form 8-K filed if material incident
- Within 4 business days of determination of materiality
- Describe nature, scope, timing
- Material impact on operations/financial condition
- Ongoing review of materiality

Industry-Specific:

- Financial: FINRA, OCC, Federal Reserve, state regulators
- Energy: TSA Pipeline Security, DOE, FERC
- Defense: DFARS requirements, CMMC
- Other: Check industry regulatory requirements

Customer Communication Strategy

Proactive Communication Approach:

Initial Notification (If Service Impacted):

None

Subject: Service Disruption Notice

Dear Valued Customer,

We are currently experiencing a service disruption due to a cybersecurity incident affecting our systems.

Status:
- [Affected Services]: Currently unavailable
- [Unaffected Services]: Operating normally
- Estimated restoration: [Timeline or "Under assessment"]

We are working around the clock with leading cybersecurity experts to restore full service. Your data security remains our top priority.

We will provide updates every [24/48 hours] or as significant developments occur.

For questions or urgent needs, contact: [Contact Information]

Thank you for your patience and understanding.

[Name, Title]

Data Breach Notification (If Data Stolen):

None

Subject: Important Notice About Your Data

Dear [Customer Name],

We are writing to inform you of a data security incident that may have affected your information.

What Happened:
On [Date], we discovered unauthorized access to our systems. An investigation has determined that certain customer data may have been accessed or stolen.

What Information Was Involved:
[Specific data types: names, email addresses, purchase history, etc. - BE SPECIFIC]

What We Are Doing:
- Immediately contained the incident and engaged cybersecurity experts
- Completed comprehensive investigation
- Implemented enhanced security measures
- Notified law enforcement and regulatory authorities
- [If applicable: Decided not to pay ransom to criminal actors]

What You Can Do:
[Specific recommendations based on data types involved]
- Monitor accounts for suspicious activity
- Consider fraud alert or credit freeze
- [If offering: Enroll in complimentary [12-month] credit monitoring service]

Additional Information:
Detailed FAQ: [Website URL]
Dedicated Call Center: [Phone Number], [Hours]
Email: [Dedicated Email Address]

We sincerely apologize for this incident and any concern or inconvenience it may cause. We take the security and privacy of your information very seriously.

Sincerely,
[CEO Name]

Ongoing Updates:

- Transparency about restoration progress
- Acknowledge customer frustration
- Provide specific timelines when possible
- Celebrate milestones (systems restored)

Return to Normal Communication:

None

Subject: Systems Fully Restored - Thank You

Dear Valued Customer,

We are pleased to inform you that all systems have been fully restored and are operating normally.

Summary:
- Incident began: [Date]
- Full restoration completed: [Date]
- Duration: [X days]
- Enhanced security measures implemented
- No evidence of data misuse (if applicable)

What's Changed:
- [New security measures customers will notice]
- [Any new procedures]
- [Improvements made]

We deeply appreciate your patience and loyalty during this challenging time.
Your trust is our most valuable asset, and we have learned important lessons that have made us stronger and more secure.

Thank you,
[CEO Name]

Media Management

If Media Inquiries Received:

Designate Single Spokesperson:

- Typically CEO or designated executive
- Media training required
- Consistent messaging

Prepared Statement:

None

"On [Date], we experienced a cybersecurity incident affecting our systems.
We immediately activated our incident response plan and engaged leading cybersecurity experts.

The security and privacy of [customer/patient/client] information is our highest priority. We have taken immediate action to contain the incident, are conducting a thorough investigation, and have notified appropriate authorities.

[If applicable: We are providing affected individuals with [credit monitoring/support services] and have established a dedicated [phone line/website] for questions.]

We have implemented enhanced security measures and will continue to invest in protecting the information entrusted to us.

We will provide updates as appropriate while respecting the ongoing investigation."

Questions to Expect:

- How many people were affected?
- What data was compromised?
- Did you pay the ransom?
- Were you in compliance with security standards?
- Have there been previous incidents?
- What will you do differently?
- Should customers be worried?

Response Strategy:

- Be honest but measured
- Don't speculate beyond known facts
- Acknowledge impact and apologize
- Focus on actions taken
- Direct to resources for affected individuals
- Don't blame employees or vendors publicly

Partner/Vendor Communication

Business Partners Need to Know:

- Potential impact on shared data
- Supply chain considerations
- Contractual notification requirements
- Reassurance about security improvements

Vendor Communication:

- Thank those who helped respond
- Review contracts for security requirements
- Consider enhanced due diligence going forward

Internal Communication

Employee Updates:

- Acknowledge their hard work during incident
- Explain what happened (appropriate level of detail)
- What's changing for them (new security measures)
- Their role in preventing future incidents
- Answer questions transparently

Town Hall Meeting:

- CEO leads discussion
- CISO provides technical overview
- Q&A session
- Reinforces security culture

4.4 Insurance Claim Finalization

Complete Documentation Package

Required Documentation:

1. Incident Timeline and Description

- Detailed narrative of incident
- Detection through resolution
- All major events with timestamps
- Decision points and rationale

2. Financial Impact Documentation

Direct Costs:

- Ransom payment (if paid) with proof:
  - Blockchain transaction records
  - Amount in USD and BTC
  - Date of payment
  - Legal authorization
- Incident response costs:
  - Forensic investigation invoices
  - Legal counsel invoices
  - Negotiation specialist invoices (if used)
  - IT recovery costs
  - Public relations costs
  - Notification costs (printing, mailing, call center)
  - Credit monitoring costs

Business Interruption:

- Revenue loss calculations
- Documentation methodology
- Historical comparison
- Industry benchmarking
- Supporting financial statements

Extra Expenses:

- Overtime costs
- Emergency hardware purchases
- Cloud resource expenses
- Contractor/consultant costs
- Travel expenses for response team

3. Technical Evidence

- Forensic investigation reports
- Malware analysis
- IOC documentation
- System restoration documentation
- Security improvements implemented

4. Communication Records

- All negotiation transcripts (if paid)
- Customer notifications sent
- Regulatory filings
- Media statements
- Internal communications

5. Third-Party Reports

- Forensic investigator final report
- Legal opinions (OFAC compliance, etc.)
- External auditor reports (if applicable)
- Regulator correspondence

Claims Process Management

Work with Insurance Adjuster:

- Provide requested documentation promptly
- Maintain open communication
- Explain decisions made
- Justify all expenses

Common Claim Issues:

Issue 1: "Failure to Maintain Reasonable Security"

Insurer Argument: "You didn't have basic controls, so we won't cover"

Your Defense:

- Document all security measures that WERE in place
- Explain resource constraints
- Show industry-standard practices were followed
- Provide evidence of security investments
- Demonstrate good faith efforts

Issue 2: "Act of War" Exclusion

Insurer Argument: "This was nation-state attack, war exclusion applies"

Your Defense:

- Attribution is extremely difficult
- Ransomware is financially motivated crime, not war
- Legal precedent unclear (this is evolving)
- May require litigation

Issue 3: "Late Notice"

Insurer Argument: "You didn't notify us fast enough, claim denied"

Your Defense:

- Demonstrate notification timeline was reasonable
- Show you notified as soon as you understood incident scope
- Provide evidence of good faith
- Policy language interpretation

Issue 4: "Betterment"

Insurer Argument: "We won't pay for upgraded systems, only restore to prior state"

Your Response:

- Technology has advanced since original purchase
- Equivalent products no longer available
- Necessary for security (not just upgrade)
- Depreciation considerations

Claim Settlement Negotiation

Expected Payout:

- Rarely 100% of claimed amount
- Typical: 70-90% of documented costs
- Negotiation is normal
- May take 6-12 months for full settlement

If Claim Disputed:

- Review policy language with attorney
- Gather additional supporting documentation
- Consider independent appraisal
- Mediation or arbitration clauses
- Litigation as last resort (expensive)

Future Premium Impact:

- Expect 20-50% premium increase on renewal
- Multiple claims may result in non-renewal
- Market conditions also affect pricing
- Shop market at renewal
- Consider higher deductibles to reduce premium

4.5 Lessons Learned and Continuous Improvement

Post-Incident Review (30-45 Days After Resolution)

Facilitated Discussion with Key Stakeholders:

Attendees:

- Executive team (CEO, CFO, COO)
- IT leadership (CIO, CISO)
- Incident response team members
- External consultants (if valuable)
- Board representative

Discussion Format:

1. What Happened? (30 minutes)
    - Chronological incident timeline
    - Key events and decisions
    - Technical details (appropriate level)
    - Impact assessment
2. What Went Well? (30 minutes)
    - Successful containment actions
    - Effective coordination
    - Good decisions made under pressure
    - Individual/team recognition
3. What Could Have Gone Better? (60 minutes)
    - Delayed responses or actions
    - Communication breakdowns
    - Resource constraints
    - Decision-making challenges
    - Technical difficulties
4. Why Did This Happen? (Root Cause) (45 minutes)
    - Technical vulnerability or weakness
    - Process failures
    - Resource/budget constraints
    - Human factors
    - Systemic issues
5. How Do We Prevent Recurrence? (60 minutes)
    - Technical improvements needed
    - Process changes required
    - Training and awareness
    - Resource requirements
    - Timeline and priorities

6. What Did We Learn? (30 minutes)

- Key takeaways for organization
- Industry insights to share
- Documentation improvements
- Playbook updates

Lessons Learned Report

Executive Summary:

- Incident overview
- Impact summary
- Key findings
- Priority recommendations
- Investment requirements

Detailed Analysis:

What Worked Well:

- Backup strategy (if applicable)
- Containment procedures
- Team coordination
- Vendor relationships
- Communication approach
- (Be specific with examples)

What Didn't Work Well:

- Delayed detection
- Incomplete backups
- Insufficient segmentation
- Credential management weaknesses
- Response plan gaps
- (Be specific with examples)

Root Causes:

- Technical: Specific vulnerability or weakness
- Process: Which process failed or didn't exist
- People: Training gaps, awareness issues
- Budget: Resource constraints that contributed

Recommendations by Priority:

Priority 1: Critical (Immediate - 30 days)

- Close initial access vector
- Eliminate persistence mechanisms
- Implement critical compensating controls
- Budget required: $_____

Priority 2: High (Short-term - 90 days)

- Major security improvements
- Process enhancements
- Training programs
- Budget required: $_____

Priority 3: Medium (Medium-term - 6 months)

- Architecture improvements
- Tool deployments
- Advanced capabilities
- Budget required: $_____

Priority 4: Low (Long-term - 12 months)

- Strategic initiatives
- Cultural changes
- Maturity improvements
- Budget required: $_____

Total Investment Required: $_____ Risk Reduction Expected: ____%

Security Improvement Roadmap

Immediate Actions (Days 1-30):

Quick Wins:

- MFA on all external access
- Disable internet-facing RDP
- Block executable email attachments
- Enable EDR on all systems
- Implement application whitelisting on servers
- Password policy strengthening
- Emergency patching of critical vulnerabilities

Short-Term Projects (Months 2-3):

Foundation Building:

- Network segmentation implementation
- PAM solution deployment (Phase 1)
- SIEM enhancement with critical detection rules
- Backup architecture improvements
- Vulnerability management program
- Incident response plan update and testing
- Security awareness training program launch

Medium-Term Projects (Months 4-6):

Capability Enhancement:

- Zero-trust architecture initiation
- PAM full deployment
- Advanced threat protection
- Deception technology deployment
- Security orchestration (SOAR)
- Threat intelligence integration
- Red team assessment

Long-Term Initiatives (Months 7-12):

Maturity Improvement:

- Security operations center (SOC) build or enhance
- Advanced analytics and AI/ML detection
- Threat hunting program
- Bug bounty program
- Security architecture transformation
- DevSecOps integration
- Continuous monitoring and improvement

Metrics and KPIs

Track Progress and Improvement:

Security Metrics:

- Mean time to detect (MTTD)
- Mean time to respond (MTTR)
- Number of high/critical vulnerabilities
- Patching compliance (% within SLA)
- MFA adoption rate
- Security training completion rate
- Phishing simulation click rate
- Security incident count and severity

Ransomware-Specific:

- Backup success rate
- Backup restoration testing frequency
- Time to restore from backup (tested)
- Coverage of immutable backups
- EDR detection rate for ransomware simulations
- Privileged account management coverage

Business Metrics:

- Security investment as % of IT budget
- Cyber insurance premium trends
- Customer trust scores
- Regulatory compliance scores
- Time to onboard new security controls

Set Targets:

- Where are we now? (Baseline)
- Where do we want to be? (Target)
- When do we want to get there? (Timeline)
- Who is accountable? (Owner)

Playbook Updates

Update Incident Response Plan:

- Incorporate lessons learned
- Update contact lists
- Refine procedures based on experience
- Add new scenarios
- Update decision trees
- Improve templates

Create Ransomware-Specific Playbook:

None

RANSOMWARE INCIDENT RESPONSE PLAYBOOK

Detection Phase:
- [Specific indicators we learned]
- [Detection sources that worked]
- [Updated response triggers]

Containment Phase:
- [Improved containment steps]
- [Updated network isolation procedures]
- [Better preservation techniques]

Analysis Phase:
- [Enhanced forensic procedures]
- [Specific tools and techniques]
- [Evidence collection checklist]

Recovery Phase:
- [Backup restoration procedures that worked]
- [System rebuild approach]
- [Validation steps]

Communication Phase:
- [Improved notification templates]
- [Stakeholder communication plan]
- [Media response strategy]

Board Presentation on Improvements

Present to Board Post-Incident (60-90 Days):

Agenda:

1. Incident Recap (10 minutes)
    - What happened
    - Impact (quantified)
    - Response actions
    - Resolution
2. Lessons Learned (15 minutes)
    - Root causes identified
    - What worked / didn't work
    - Key insights
3. Investment Proposal (20 minutes)
    - Prioritized improvements
    - Budget requirements by priority
    - Risk reduction for each investment
    - Timeline for implementation
4. Governance Improvements (10 minutes)
    - Enhanced oversight
    - Regular reporting
    - Risk dashboard
    - Board cyber education
5. Long-Term Strategy (10 minutes)
    - Vision for security posture
    - Industry leadership
    - Continuous improvement
    - Culture change
6. Q&A (15 minutes)

Request Board Approval:

- Budget for Priority 1 & 2 items (minimum)
- Authority to proceed with implementations
- Commitment to ongoing investment
- Board-level security committee (if don't have)

Organizational Change Management

Culture Shift Required:

From Reactive to Proactive:

- Security as enabler, not blocker
- Prevention-first mindset
- Continuous improvement culture
- Shared responsibility for security

Change Management:

- Executive sponsorship (CEO champion)
- Clear vision and strategy
- Communication plan
- Training and enablement
- Measure and celebrate progress
- Recognize and reward security behaviors

Long-Term Resilience:

- Regular testing (tabletops, red teams)
- Continuous improvement process
- Industry engagement and learning
- Investment in people and technology
- Adaptability to evolving threats

PHASE 5: SPECIAL CONSIDERATIONS

5.1 Reinfection Scenarios

The Harsh Reality: **80%** of organizations that pay ransoms are **attacked again within 12 months.**

Why Reinfection Happens

1. Same Threat Actor Returns
    - They know you paid (you're a good target)
    - Initial access vector not closed
    - Persistence mechanisms remain
    - They sold your access to other criminals
    - Different "affiliate" of same RaaS operation
2. Different Threat Actor
    - Your vulnerability is publicly known
    - Other groups scan for same weakness
    - Word spreads in criminal forums
    - Compromised credentials sold on dark web
3. Insider Knowledge
    - They mapped your network
    - They know your security gaps
    - They know your backup strategy
    - They know your response capability
    - They have detailed intelligence on you

Preventing Reinfection

Critical Requirements:

1. Complete Remediation (Not Partial)
    - Every persistence mechanism eliminated
    - Every credential rotated
    - Every vulnerability patched
    - Initial access vector 100% closed
    - Forensics confirmed complete scope
2. Architecture Change
    - Can't just restore to previous state
    - Must implement hardening improvements
    - Network segmentation essential
    - Zero-trust approach
    - Assume breach mentality

3. Enhanced Detection
    - They'll try to be stealthy
    - Need better visibility than before
    - Behavioral analytics
    - Threat hunting
    - 24/7 monitoring
4. Continuous Validation
    - Regular penetration testing
    - Red team exercises
    - Assume they're trying to get back in
    - Active defense posture

If Reinfection Occurs

DO NOT PAY AGAIN

Why:

- Paying twice establishes you as permanent target
- They'll keep coming back
- Each payment funds more sophisticated attacks
- Become known as "easy mark" in criminal forums

Response to Reinfection:

1. Immediate Assessment
    - Same threat actor or different?
    - Same method or new?
    - How did forensics miss it?
2. More Aggressive Response
    - Complete environment rebuild (no restore)
    - Assume everything is compromised
    - Fresh Active Directory domain
    - New network architecture
    - Zero trust from endpoints
3. External Expertise
    - Engage different IR firm (fresh perspective)
    - Red team to find remaining weaknesses
    - Architecture review
    - Assume initial remediation was insufficient
4. Accept Business Impact
    - Longer downtime for complete rebuild
    - Higher costs
    - But breaks reinfection cycle
    - Demonstrates to criminals you won't keep paying

5.2 Multiple Simultaneous Attacks

Emerging Threat: Coordinated attacks from multiple ransomware groups

Why This Happens

Your data/access was sold:

- Initial attacker sold credentials to others
- Multiple groups enter through different vectors
- Race to encrypt and ransom first
- Or coordinated for maximum pressure

Response Strategy

1. Identify All Attackers
    - Different ransomware families?
    - Different communication channels?
    - Different ransom notes?
    - Timeline of infections
2. Prioritize Response
    - Most critical systems first
    - Don't negotiate with multiple groups
    - Choose recovery path instead (if possible)
    - If must pay, negotiate with most credible group only
3. Enhanced Forensics
    - Multiple initial access vectors?
    - Shared infrastructure?
    - Timeline analysis
    - Complete compromise assessment

5.3 Nation-State Attacks Disguised as Ransomware

Critical Recognition: Some "ransomware" is actually destructive attack

Warning Signs

Suspicious Indicators:

- No functional communication channel
- Implausibly high ransom (e.g., $500M)
- Timing around geopolitical events
- Targets align with nation-state interests
- Technical analysis shows no real decryption capability
- Destruction of data rather than encryption
- Wiper malware with ransom note added

Historical Examples:

- NotPetya (2017) - Russian attack on Ukraine, spread globally
- Olympic Destroyer (2018) - Attack on Olympics
- Various Iranian attacks disguised as ransomware

Response Approach

1. Immediate Recognition
   - Engage national security experts
   - Report to CISA (if critical infrastructure)
   - Don't pay (they can't/won't decrypt)
   - Treat as destructive attack
2. Different Recovery Strategy
   - No negotiation possible or useful
   - Complete rebuild required
   - Focus on business continuity
   - Forensics for attribution (government interest)
3. Different Stakeholder Engagement
   - Government agencies (FBI, CISA, NSA)
   - Industry ISACs
   - International coordination
   - Public attribution may occur

5.4 Healthcare and Life-Safety Scenarios

Special Considerations When Lives Are at Risk

Unique Ethical Considerations

Patient Safety First:

- Different calculus than pure business
- Life safety supersedes normal decision framework
- Regulatory requirements (HIPAA, patient safety regulations)
- Ethical obligations to patients

Rapid Decision Framework

Immediate Questions:

1. Are critical life-safety systems affected? (ICU monitors, ventilators, medication pumps)
2. Can we provide safe care without systems? (paper charts, manual processes)
3. How long until patient safety is compromised? (hours, days?)
4. Can we transfer patients to other facilities?
5. Is payment necessary to restore safe care quickly?

Response Approach

If Patient Safety Immediately Threatened:

- Payment decision may need to be faster (hours, not days)
- Different risk tolerance
- Board authorization may be expedited
- Document decision rationale carefully

If Safe Care Possible Without Systems:

- Activate manual procedures
- Transfer patients if needed
- Follow standard decision framework
- Don't let threat actor pressure create false urgency

Regulatory Considerations:

- Report to HHS immediately (HIPAA)
- Report to state health department
- Report to CMS (if participation affected)
- Patient notification requirements

Prevention Focus

Healthcare-Specific Security:

- Medical device security
- Network segmentation (clinical vs. administrative)
- Backup clinical systems
- Manual procedure preparedness
- Regular drills
- Redundant critical systems

5.5 Small Business / Limited Resources

Realistic Approach for Organizations Without Deep Pockets

The Reality

Small businesses face:

- Limited IT staff (or none)
- Limited budget
- May lack cyber insurance
- Can't afford expensive IR firms
- Existential threat from ransomware

Free/Low-Cost Resources

Incident Response:

- FBI Cyber Squad (free assistance)
- MS-ISAC (for state/local government and education)
- Industry ISACs (some offer help to members)
- Local FBI InfraGard chapter
- Pro-bono cyber clinic (some regions)

Prevention:

- Microsoft Defender (included with Windows)
- Free backup solutions (Windows Backup, cloud free tiers)
- CISA cyber hygiene services (free)
- No More Ransom decryptors (free)
- OpenDNS/Cloudflare (free DNS filtering)

Training:

- CISA free training materials
- KnownBe4 free phishing tests (limited)
- SANS free resources
- YouTube security training content

Realistic Prevention for SMB

Minimum Viable Security:

1. Offline Backups (CRITICAL)
    - External hard drives, disconnected daily
    - Cloud backup with versioning
    - Test restoration monthly
2. Basic Access Controls
    - MFA on email (free with Office 365, Google)
    - Strong passwords
    - Least privilege
    - Disable unnecessary accounts
3. Email Security
    - Block executable attachments
    - Anti-phishing training
    - Verify financial requests via phone
4. Patch Critical Systems
    - Enable auto-update where possible
    - Monthly security updates
    - Focus on internet-facing systems
5. Endpoint Protection
    - Microsoft Defender (free, enable tamper protection)
    - Or free solutions: Sophos Home, Bitdefender Free

Budget Priority:

- Cyber insurance (if can afford, even basic policy)
- Managed backup solution
- Managed security service (if possible)
- Annual security assessment

If Attacked (SMB Response)

Immediate Actions:

1. Unplug affected devices from network
2. Don't pay immediately (even if pressure)
3. Contact FBI (free assistance)
4. Check No More Ransom for free decryptor
5. Contact cyber insurance (if have)
6. Assess backups

If Must Pay:

- Typically see demands of $5K-$50K for small businesses
- Negotiate hard (they know you're small)
- Use cryptocurrency exchange (Coinbase easiest)
- Get legal advice (many offer free initial consultation)
- OFAC check (free on OFAC website)

Recovery:

- Restore from backups if possible
- Manual operations temporarily
- Rebuild critical systems first
- Free help from FBI, MS-ISAC, local consultants

Who is SOCRadar?

SOCRadar provides Extended Threat Intelligence (XTI) that combines: **"Cyber Threat Intelligence, Brand Protection, External Attack Surface Management, and Dark Web Radar Services."** SOCRadar provides the actionable and timely intelligence context you need to manage the risks in the transformation era.

Trusted by **21.000+ companies in 150+ countries**

Dark Web Monitoring: SOCRadar's fusion of its unique Dark Web recon technology with the human analyst eye further provides in-depth insights into financially-targeted APT groups and the threat landscape.

Protecting Customers' PII: Scan millions of data points on the surface, deep and Dark Web to accurately identify the leakage of your customers' Personally Identifiable Information (PII) in compliance with regulations.

Credit Card Monitoring: Enhance your fraud detection mechanisms with automation speed by identifying stolen credit card data on popular global black markets, carding forums, social channels, and chatters.

360-Degree Visibility: Achieve digital resilience by maintaining internet-facing digital asset inventory. Significantly accelerate this process by automated discovery, mapping, and continuous asset monitoring.

GET ACCESS FOR FREE

START YOUR FREE TRIAL

Discover SOCRadar's powerful tools and easy-to-use interface to enhance cyber threat intelligence efforts. Schedule a demo with our experts to see it in action, and we'll show you what SOCRadar can do.